SMALL SOLUTIONS TO LINEAR CONGRUENCES AND HECKE EQUIDISTRIBUTION

ANDREAS STRÖMBERGSSON AND AKSHAY VENKATESH

1. Introduction

The purpose of the present note is to give an explicit application of equidistribution of Hecke points to the problem of small solutions of linear congruences modulo primes. Let p be an odd prime. For a random system of d linear congruences in n variables modulo p, we shall ask how many "small" solutions it has, i.e. solutions in $\mathbb{Z}$ of size about $p^{d/n}$, the natural limiting point. We will show that the answer has a limit distribution as $p \to \infty$.

Questions of a similar flavour for varieties of higher degree have been studied, i.e. given an affine variety $V \subset \mathbb{A}^n$ over $\mathbb{Z}/p\mathbb{Z}$ of codimension d, it may be regarded as defining a system of polynomial congruences for n integers $(x_1, \ldots, x_n) \in \mathbb{Z}^n$. One can ask (if very optimistic) whether there always exists an integral solution so that $\max_{1 \leqq i \leqq n} |x_i| \leqq Cp^{d/n}$, for some constant C depending only on the invariants of V, e.g. degree. This is easily seen to be false, but it turns out that one may prove weaker assertions of this nature: see, for example, [L]. The present note shows that in the seemingly easy case of linear varieties, the small solutions exhibit interesting statistical properties which are, somewhat surprisingly, related to automorphic forms.

The question of small solutions of linear congruences is also closely related to the study of fractional parts of linear forms (cf. Section 7 below), which have been investigated by a number of authors using ergodic theory: see, e.g., Marklof [M1]. In our context, we shall use automorphic forms and spectral theory in place of ergodic theory; we are therefore able to give explicit error estimates.

The application of the spectral theory of automorphic forms to certain Diophantine questions in number theory is not new; see, for instance, Sarnak's ICM address [Sa2]. Hecke equidistribution in particular has been studied in great generality by Clozel, Oh and Ullmo in [COU]. Our problem involves passing from smooth to sharp cutoff test functions in the equidistribution results; for this we give a simple way of optimizing the harmonic

2000 *Mathematics Subject Classification.* Primary 11P21; Secondary 11F70.

A.S. was supported by a Swedish STINT Postdoctoral award.
A.V. was supported by NSF grant DMS-0245606.

analysis (Section 2). Our methods here allow us to get sharper error estimates than previous authors (see comments after Theorem 2). The application of Hecke equidistribution on $\mathrm{SL}_n(\mathbb{R})$ to the case of homogeneous linear congruences is carried out in Section 3.

We will also make use of the *non-reductive* group $\mathrm{SL}_n(\mathbb{R}) \ltimes \mathbb{R}^n$, and establish some results about its spectrum that may be of independent interest. (Similar non-reductive groups have found applications in other works which use ergodic theory, for example [EM] and [M2]; the spectral bounds that we discuss here allow for error estimates, and we hope they will be useful in other contexts.) These results are established in Section 4 and applied to the statistics of inhomogeneous linear congruences in Section 5.

In the case of $\mathrm{SL}_2(\mathbb{R}) \ltimes \mathbb{R}^2$ we go further. By explicit geometric considerations we show how to obtain a better error term than is obtainable by "general representation-theoretic considerations" (Section 6). This involves a careful analysis of the smoothness at the boundary for several subsets of $\mathrm{SL}_2(\mathbb{R}) \ltimes \mathbb{R}^2$.

We now give a typical result; prior to doing so, we fix some notation that will be valid throughout the paper. Firstly, recalling that p will always denote an odd prime, we will repeatedly identify $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ with the set $\{-\frac{p-1}{2}, -\frac{p-3}{2}, \dots, \frac{p-1}{2}\}$. Correspondingly, we will identify $\mathbb{F}_p^r = (\mathbb{Z}/p\mathbb{Z})^r$ with the set $\{-\frac{p-1}{2}, -\frac{p-3}{2}, \dots, \frac{p-1}{2}\}^r$. Secondly, by *affine line* or *affine hyperplane* in a vector space V we mean a translate of a (usual) line or hyperplane; thus, for instance, the linear congruence $x + y + z \equiv 1 \pmod{p}$ defines an affine hyperplane in $(\mathbb{Z}/p\mathbb{Z})^3$. With these conventions:

Theorem 1. *Let $K > 0$ be fixed. Let p be a prime, and B the subset of $(\mathbb{Z}/p\mathbb{Z})^3$ defined by $\{|x_i| \leqq Kp^{2/3}, 1 \leqq i \leqq 3\}$. There are real positive constants c_r, for r a non-negative integer, with the property that $\sum_{r=0}^{\infty} c_r = 1$, and so that the number of affine lines in $(\mathbb{Z}/p\mathbb{Z})^3$ that intersect B in precisely r points is $c_r p^4(1 + O_r(p^{-1/12}))$.*

Thus the probability that a system of two linear congruence $a_1x + b_1y + c_1z \equiv d_1$, $a_2x + b_2y + c_2z \equiv d_2 \pmod{p}$ has exactly r solutions in the box $(x, y, z) \in [-Kp^{2/3}, Kp^{2/3}]^3$ converges to c_r as $p \to \infty$. Note that one could also make the implicit constant in $O(p^{-1/12})$ explicit.

The corresponding statement for usual (non-affine) lines in $(\mathbb{Z}/p\mathbb{Z})^3$ (i.e. lines passing through $(0, 0, 0)$) is significantly easier, as it only uses SL_3.

This theorem holds (with the appropriate modifications) for affine hyperplanes of any dimension in any $(\mathbb{Z}/p\mathbb{Z})^n$. In the case $n = 2$ we have determined the constants c_r explicitly for r or K small, by explicit computation of the relevant volumes in $\mathrm{SL}_2(\mathbb{R}) \ltimes \mathbb{R}^2$ (as well as in $\mathrm{SL}_2(\mathbb{R})$, for the case of homogeneous congruences), see Section 8. The formulas obtained generalize results of Mazel and Sinai [MS] in the context of Diophantine approximation (cf. Section 7). It is interesting to note that the c_r do not vary smoothly with K, the parameter that controls the size of the box; a similar phenomenon occurs in [EM].

Our approach of course owes much to previous authors. The notion of "smooth set" that we use appeared (in the notion of "well-rounded") in the paper [EsM] of Eskin-McMullen. The estimates in Hecke operators that are used in Section 3 are already in [COU], and Sobolev norms are used elegantly in [GO]. The computations in Section 8 are inspired by the method of Elkies and McMullen [EM, pp. 30–37].

We would like to thank T. Ekholm, J. Marklof, S. Janson and P. Sarnak for useful and inspiring discussions.

2. Harmonic Analysis on Lie Groups

The material in this section contains no essential new ideas; we do however note in Lemma 2 a very simple method for obtaining essentially sharp (within ε) pointwise estimates for functions in terms of their Sobolev norms without explicit interpolation. This will later allow us to get better estimates for Hecke equidistribution with sharp cutoff functions than previous authors (cf. Theorem 2).

Let G be a real Lie group, $\Gamma \subset G$ a lattice. Fix a basis $\{X_i\}$ for the Lie algebra of G. If V is any unitary G-representation, we define the Sobolev norm

$$S_k(v) = \sqrt{\sum_{\mathrm{ord}(D) \leqq k} ||Dv||_2^2}, \tag{1}$$

the sum being over all monomials in the X_i of degree $\leqq k$. This norm depends on the choice of basis only up to a constant; in each of our applications, we will regard a basis $\{X_i\}$ as having been fixed for all time, and we will make use of it without explicit mention.

Throughout this paper, by *representation* we mean *unitary representation*.

If X is a metric space, $S \subset X$, and $\delta > 0$, we set $B(S, \delta)$ to be the δ-neighbourhood of S in X. We further set $(\partial_\varepsilon S) = B(S, \varepsilon) \cap B(X - S, \varepsilon)$.

If X is a metric space endowed with a measure ν, we say a subset $S \subset X$ is K-*smooth* if $\nu(\partial_\varepsilon S) \leqq K\varepsilon$ (this being assumed for $\varepsilon \leqq 1$, say). We say it is *smooth* if it is K-smooth for some K.

Finally, suppose X that is as above (a metric space endowed with measure ν), and additionally suppose that it is a smooth manifold and G acts on X smoothly and in a measure-preserving fashion. Then $L^2(X)$ is a unitary G-representation. If $f \in C^\infty(X)$ is any smooth function, we may define the k-Sobolev norm $S_k(f)$ formally according to (1), even if f or its derivatives do not belong to $L^2(X)$; with this definition it is possible that $S_k(f) = \infty$.

To avoid confusion, we denote by μ a Haar measure on G and vol the standard Lebesgue measure on $\mathbb{R}^n$. For definiteness, we will normalize so that $\mu(\Gamma \backslash G) = 1$.

We now set $X = \Gamma \backslash G$. We fix a Riemannian metric d on G, left invariant for the G-action. Let U_ε be the ε-neighbourhood of $1 \in G$. The metric d descends to a Riemannian metric on $X = \Gamma \backslash G$ that we also denote by d.

In particular, for $x, y \in X$, one has $d(x,y) < \varepsilon$ if and only if $x \in yU_\varepsilon$. We endow X with the G-invariant measure with total mass 1. As above, we have a notion of Sobolev norm $S_k(f)$ for $f \in C^\infty(X)$.

For each $\delta \leqq 1$ we fix k_δ to be a positive smooth compactly supported test functions on G, so that:

(1) $\int_G k_\delta(g)dg = 1$;
(2) $\int_G |Dk_\delta(g)|dg \ll_j \delta^{-j}$ for any D, a monomial in the X_is of order j;
(3) Supp $k_\delta \subset U_\delta$.

Our first lemma concerns approximating the characteristic function of a smooth set by C^∞ functions. Let us recall that if G acts on the space X and f is a function on X, we define the convolution $f \star k_\delta(x) = \int_{g\in G} f(xg)k_\delta(g^{-1})dg$.

Lemma 1. *Let $T \subset X$ be K-smooth, and let e_T be its characteristic function. For each $0 < \delta \leqq 1/2$ there exist functions $e_{-,\delta}$ and $e_{+,\delta}$ in $C^\infty(X)$ so that for all $j \geqq 1$ one has:*

$$0 \leqq e_{-,\delta} \leqq e_T \leqq e_{+,\delta} \leqq 1; \tag{2}$$

$$S_j(e_{-,\delta}), S_j(e_{+,\delta}) \ll K^{1/2}\delta^{1/2-j}; \tag{3}$$

$$||e_{\pm,\delta}(x) - e_T(x)||_{L^1} \leqq 2K\delta. \tag{4}$$

Proof. Let $T_- = T - (\partial_\delta T)$ and $T_+ = T \cup \partial_\delta T$.

Now set e_{T_-} to be the characteristic function of T_-, and set $e_{-,\delta} = e_{T_-} \star k_\delta$; similarly define $e_{+,\delta}$. It is easy to see the first and last conditions.

Let D be any monomial in the X_is of degree $\leqq j$. Then $De_{-,\delta} = e_{T_-} \star (Dk_\delta)$ is supported in a 2δ-neighbourhood of the boundary of T, in particular a set of volume $\leqq 2K\delta$; further $||De_{-,\delta}||_\infty \leqq \int_G |Dk_\delta(g)|dg \ll_j \delta^{-j}$. One obtains immediately the stated result. □

The following lemma allows us to give an almost sharp (to within ε) pointwise bound of Sobolev type.

Lemma 2. (Pointwise bounds) *Let $M = \dim(G)/2$. Let $k = [M]$ and $\{M\} = M - k$. Let $x \in X$ and $f \in C^\infty(X)$. Then*

$$f(x) \ll_{x,\varepsilon} S_k(f)^{1-\{M\}-\varepsilon} S_{k+1}(f)^{\{M\}+\varepsilon}.$$

Proof. Indeed, by choosing a coordinate chart, it suffices to prove it for $\mathbb{R}^n$, where the result follows (for example) from Hölder's inequality and the usual Sobolev estimate. □

It is more precise and more canonical to use interpolation (in fact, evidently the lemma above is an approximate form of interpolation). However, this very simple lemma allows us to get estimates that are just as good with a minimum of technical overhead!

We now give a variant of Lemma 1, needed in Section 6 below. Specifically, the above lemma concerned approximation of a characteristic function by smooth functions. The next lemma concerns approximation of functions that have (roughly speaking) one more derivative of smoothness than a characteristic function (e.g. the absolute value function on $\mathbb{R}$).

Lemma 3. *Let $f : X \to \mathbb{R}$ be a continuous function such that for some positive constants $K, C, C_1, C_2, \ldots$, the following assumptions hold:*
(i) $|f(x) - f(y)| \leqq C \cdot d(x,y)$ for all $x, y \in X$; (ii) there is a K-smooth closed subset $S \subset X$ of measure 0 such that $f \in C^\infty(X - S)$; (iii) $|Df(x)| \leqq C_j \delta^{1-j}$ for each monomial D in the X_i's of order $j \geqq 1$ and all $0 < \delta < 1$, $x \in X - B(S,\delta)$.

Then for each $0 < \delta < \frac{1}{2}$ there exist functions $e_{-,\delta}$ and $e_{+,\delta}$ in $C^\infty(X)$ such that:

$$e_{-,\delta} \leqq f \leqq e_{+,\delta}; \tag{5}$$

$$S_j(e_{-,\delta}), S_j(e_{+,\delta}) \ll \begin{cases} 1 & \text{for } j = 1 \\ \delta^{3/2-j} & \text{for } j \geqq 2; \end{cases} \tag{6}$$

$$||e_{\pm,\delta} - f||_{L_1} \ll \delta^2 \log(\delta^{-1}). \tag{7}$$

(The implied constants depend only on the constants $K, C, C_1, C_2, \ldots$, and on j.)

Proof. The idea is to smooth f by convolving it with a k_δ, and then to modify the result so as to ensure that it is either larger than or less than f.

Applying Taylor's formula to the function $t \mapsto f(x \exp tY)$ for $x \in X$ and Y in the Lie algebra of G, and using (iii) for $j = 2$, we find that there is a constant $C_1 = C_1(f) > 0$ such that for all sufficiently small $\delta_1 > 0$ and all $x \in X - B(S,\delta_1)$, $\delta \in (0, \delta_1/2]$,

$$\left|\tfrac{1}{2}\big(f(xg) + f(xg^{-1})\big) - f(x)\right| \leqq C_1 \delta_1^{-1} \delta^2, \qquad \forall g \in U_\delta \subset G. \tag{8}$$

We increase C_1, if necessary, so that (8) holds whenever $0 < 2\delta \leqq \delta_1 \leqq 1$. Now let k_δ be as before, and impose the extra assumption that $k_\delta(g^{-1}) = k_\delta(g)$ for all $g \in G$. We then have $f \star k_\delta(x) = \frac{1}{2}\int_G \big(f(xg) + f(xg^{-1})\big) k_\delta(g)\, dg$, and hence by (8), if $0 < 2\delta < \delta_1 \leqq 1$,

$$\big|f \star k_\delta(x) - f(x)\big| \leqq C_1 \delta_1^{-1} \delta^2, \qquad \forall x \in X - B(S,\delta_1). \tag{9}$$

We also have, because of (i),

$$\big|f \star k_\delta(x) - f(x)\big| \leqq C\delta, \qquad \forall x \in X. \tag{10}$$

Now let $0 < \delta < \frac{1}{2}$ be given. For any monomial $D = X_{i_1} \ldots X_{i_j}$ $(j \geqq 1)$ we have by (i) and (ii),

$$\begin{aligned} D[f \star k_\delta](x) &= X_{i_1}\big[f \star X_{i_2} \ldots X_{i_j} k_\delta\big](x) \\ &= \int_G (\mathrm{Ad}(h) X_{i_1}) f(xh^{-1}) \cdot X_{i_2} \ldots X_{i_j} k_\delta(h)\, dh. \end{aligned}$$

But $\{\mathrm{Ad}(h)(X_{i_1}) \mid h \in U_{\frac{1}{2}}\}$ is a compact subset of the Lie algebra of G, and hence $||D(f \star k_\delta)||_\infty \ll \delta^{1-j}$. Similarly, if $x \notin B(S, 2\delta)$ we have $D[f \star k_\delta](x) = \int_G (\mathrm{Ad}(h)D) f(xh^{-1}) \cdot k_\delta(h)\, dh$, and hence, writing $M = [\log_2 \delta^{-1}] \in \mathbb{Z}^+$ and using (iii), we have $D[f \star k_\delta](x) \ll_j (2^m\delta)^{1-j}$ for all $m = 1, 2, ..., M$ and all $x \in X - B(S, 2^m\delta)$. Using these bounds and decomposing X into the regions $B(S, 2\delta)$, $B(S, 2^{m+1}\delta) - B(S, 2^m\delta)$ for $m = 1, 2, ..., M$, and $X - B(S, 2^{M+1}\delta)$ (which have measures $\ll \delta$, $\ll 2^m\delta$ and $\ll 1$, respectively), we obtain

$$S_j(f \star k_\delta) \ll \begin{cases} 1 & \text{if } j = 1 \\ \delta^{3/2-j} & \text{if } j \geqq 2. \end{cases} \tag{11}$$

For any $\delta_1 > 0$ we define $u_{\delta_1} = 1_{B(S,2\delta_1)} \star k_{\delta_1}$, and let

$$e_{\pm,\delta} = f \star k_\delta \pm \max(C, C_1)\Big(\delta^2 + \delta \sum_{m=1}^{M+1} 2^{1-m} u_{2^m\delta}\Big).$$

Note that $0 \leqq u_{\delta_1} \leqq 1$ and $u_{\delta_1}(x) = 1$ for all $x \in B(S, \delta_1)$. Hence (5) follows easily from (9) and (10). Furthermore, arguing as in the proof of Lemma 1, we find that $S_j(u_{\delta_1}) \ll_{j,K} \delta_1^{\frac{1}{2}-j}$ for each $j \geqq 1$ and $0 < \delta_1 < 10$. Combining this with (11), we obtain (6). Finally, decomposing X as before and using (9), (10) we find that $||f \star k_\delta - f||_1 \ll \delta^2 \log(\delta^{-1})$. We also have $||u_{\delta_1}||_1 \leqq ||1_{B(S,3\delta_1)}||_1 \ll \delta_1$ for $0 < \delta_1 < 10$. Hence we obtain (7). □

3. Homogeneous linear congruences

Let Ω be a compact subset of $\mathbb{R}^n$. We shall assume that Ω contains a neighbourhood of the origin, and that Ω satisfies a certain mild smoothness condition (see below). For instance, if $K > 0$, the sets $\Omega = \{(x_1, \ldots, x_n) : \sum_i |x_i|^2 \leqq K\}$ or $\Omega = \{(x_1, \ldots, x_n) : |x_j| \leqq K \text{ for all } 1 \leqq j \leqq n\}$ are both certainly admissible.

We shall now study how many solutions a system of j linear congruences mod p has in the set $p^{j/n}\Omega$; the final result is stated in Theorem 2.

Set in this section $\Gamma = \mathrm{SL}_n(\mathbb{Z}), G = \mathrm{SL}_n(\mathbb{R}), X = \Gamma\backslash G$. As usual, $\Gamma\backslash G$ is identified with the moduli space of unimodular rank n lattices, via $g \mapsto \mathbb{Z}^n g$.

3.1. Hecke operators for SL_n.

Let $T_{p,j}$ be the jth Hecke operator at p, explicitly described as follows: if L is a lattice, $T_{p,j}$ is the following formal linear combination of lattices:

$$T_{p,j} = \frac{\sum_{L/L' \equiv (\mathbb{Z}/p)^j} [\frac{1}{p^{j/n}} L']}{\sum_{L'} 1}.$$

$T_{p,j}$ induces a correspondence from $\mathrm{SL}_n(\mathbb{Z})\backslash\mathrm{SL}_n(\mathbb{R})$ to itself, whereby it induces an endomorphism of $L^2(\mathrm{SL}_n(\mathbb{Z})\backslash\mathrm{SL}_n(\mathbb{R}))$; we shall use the notation $T_{p,j}$ to also denote this endomorphism. To compute the operator norms of the $T_{p,j}$, we invoke some representation theory. Let μ_{T_j} be the restriction of Haar measure to the following $\mathrm{GL}_n(\mathbb{Z}_p)$-double coset in $\mathrm{GL}_n(\mathbb{Q}_p)$:

$$\mathrm{GL}_n(\mathbb{Z}_p)\mathrm{diag}(p^{-1}, p^{-1}, \ldots, p^{-1}, 1, \ldots, 1)\mathrm{GL}_n(\mathbb{Z}_p). \tag{12}$$

We normalize μ_{T_j} so its total mass is 1. Here $\mathrm{diag}(a_1,\ldots,a_n)$ refers to the diagonal matrix with entries $a_1,a_2,\ldots,a_n$, and there are exactly j p^{-1}s in the matrix $\mathrm{diag}(p^{-1},p^{-1},\ldots,p^{-1},1,\ldots,1)$.

It is then easy to verify that the action of $T_{p,j}$ corresponds (in the adelic viewpoint) to the action of μ_{T_j}. (To be precise, identify $\mathrm{SL}_n(\mathbb{Z})\backslash\mathrm{SL}_n(\mathbb{R})$ with $\mathrm{PGL}_n(\mathbb{Z})\backslash\mathrm{PGL}_n(\mathbb{R})$. This latter space may be identified with $\mathrm{PGL}_n(\mathbb{Q})\backslash\mathrm{PGL}_n(\mathbb{A})/K_f$, where $\mathbb{A}$ is the ring of adeles of $\mathbb{Q}$ and $K_f = \prod_p \mathrm{PGL}_n(\mathbb{Z}_p)$, where p ranges over finite places. Using this, one sees that a $\mathrm{GL}_n(\mathbb{Z}_p)$-bi-invariant measure on $\mathrm{GL}_n(\mathbb{Q}_p)$ acts on $L^2(\mathrm{SL}_n(\mathbb{Z})\backslash\mathrm{SL}_n(\mathbb{R}))$.)

It is also known, cf. [T], [O] that the operator norm of μ_{T_j} on any irreducible representation of $\mathrm{GL}_n(\mathbb{Q}_p)$ that is not one-dimensional is bounded above by $c_n p^{-\min(j,n-j)/2}$ if $n>2$; here c_n depends only on n. If $n=2$ there is no such upper bound owing to the absence of property (T).

$T_{p,j}$ acts on $L^2(\Gamma\backslash G)$. Let $L^2_0(\Gamma\backslash G)$ be the orthogonal complement of the constants. We define for $1 \leqq j \leqq n-1$ and $n \geqq 2$:

$$\beta(j,n) = \begin{cases} -1/2 + 7/64, j=1, n=2 \\ -\min(j,n-j)/2, n>2. \end{cases} \tag{13}$$

Then, by the above remarks (for $n>2$) and by the work of Kim and Sarnak [KS] (for $n=2$) the operator norm of $T_{p,j}$, acting on $L^2_0(\Gamma\backslash G)$ is $\ll_n p^{\beta(j,n)}$. (Implicitly, we are using the fact that the orthogonal complement of the constants in $L^2(\mathrm{PGL}_n(\mathbb{Q})\backslash\mathrm{PGL}_n(\mathbb{A}))$ does not weakly contain any 1-dimensional $\mathrm{GL}_n(\mathbb{Q}_p)$-subrepresentation; we omit the easy proof, cf. the proof of Lemma 8 below.)

3.2. **Homogeneous linear congruences and lattices.** Set $\tilde{\Omega}_r = \{g \in \mathrm{SL}_n(\mathbb{Z})\backslash\mathrm{SL}_n(\mathbb{R}) : |\mathbb{Z}^n g \cap \Omega| = r\}$. We must first ascertain that $\tilde{\Omega}_r$ does not have too badly behaved a boundary. Recall that the Haar measure μ is normalized so that $\mu(\mathrm{SL}_n(\mathbb{Z})\backslash\mathrm{SL}_n(\mathbb{R})) = 1$.

Lemma 4. *Suppose Ω is smooth (w.r.t. Lebesgue measure) and contains a neighbourhood of the origin. Then $\tilde{\Omega}_r$ is also smooth (w.r.t. Haar measure).*

Proof. Take $0<\varepsilon<1$. Let U_ε be an ε-neighbourhood of the identity in $\mathrm{SL}_n(\mathbb{R})$. Suppose $g \in \partial_\varepsilon \tilde{\Omega}_r$. Then there exist $u,u' \in U_\varepsilon$ so that $gu \in \tilde{\Omega}_r$ and $gu' \notin \tilde{\Omega}_r$.

It follows $|\mathbb{Z}^n g \cap \Omega u^{-1}| = r$ and $|\mathbb{Z}^n g \cap \Omega u'^{-1}| \neq r$. There is a constant C (depending on how large Ω is) so that the symmetric difference of Ωu^{-1} and $\Omega u'^{-1}$ is contained in $\partial_{C\varepsilon}\Omega$. (Indeed, if $h \in U_\varepsilon$ and $x \in \mathbb{R}^n$, one has $||xh - x|| \ll \varepsilon ||x||$.)

In particular the lattice $\mathbb{Z}^n g$ must contain a point in $\partial_{C\varepsilon}\Omega$. Note that for ε sufficiently small, $\partial_{C\varepsilon}\Omega$ does not contain the origin. By Siegel's theorem (see [Si], Lecture XV) the Haar measure of the set of such g is at most $\mathrm{vol}(\partial_{C\varepsilon}\Omega) = O(\varepsilon)$. $\square$

Lemma 5. *Let Ω satisfy the same hypotheses as in Lemma 4. Let $\beta(j,n)$ be as in (13) and let $\varepsilon > 0$. Then the number of Hecke translates (under $T_{p,j}$) of $\mathbb{Z}^n$ that lie in $\tilde{\Omega}_r$ is*

$$\mu(\tilde{\Omega}_r) + O_{\Omega,r,\varepsilon}(p^{\frac{2\beta(j,n)}{n^2}+\varepsilon}).$$

Proof. We have seen that $\tilde{\Omega}_r$ is smooth.

Let f be an arbitrary smooth L^1 function on $\mathrm{SL}_n(\mathbb{Z})\backslash\mathrm{SL}_n(\mathbb{R})$, set $f_0 = f - \int_{\Gamma\backslash G} f\,d\mu$, and $k = [\frac{n^2-1}{2}], \alpha = \frac{n^2-1}{2} - k$. The operator norm of $T_{p,j}$, considered as an endomorphism of $L^2_0(\Gamma\backslash G)$ with the usual norm, bounds from above the operator norm of $T_{p,j}$ considered as an endomorphism of the corresponding k-Sobolev spaces (i.e. the completion of the space of smooth vectors in $L^2_0(\Gamma\backslash G)$ w.r.t. S_k). This is a straightforward deduction from the fact that $T_{p,j}$ commutes with the G-action; in fact the norms are equal, but we do not need this.

Combining this, Lemma 2, and the definition of $\beta(j,n)$ (see (13) and the remarks that follow), we obtain:

(14)
$$T_{p,j}f(\mathbb{Z}^n) - \int_{\Gamma\backslash G} f\,d\mu = T_{p,j}f_0(\mathbb{Z}^n) \ll_\varepsilon p^{\beta(j,n)} S_k(f_0)^{1-\alpha-\varepsilon} S_{k+1}(f_0)^{\alpha+\varepsilon}.$$

Let $e_{\tilde{\Omega}_r}$ be the characteristic function of $\tilde{\Omega}_r$. We have seen in Lemma 1 that one may approximate $e_{\tilde{\Omega}_r}$ from above and below by smooth functions $e_{\tilde{\Omega}_r,\pm,\delta}$. We apply (14) with $f = e_{\tilde{\Omega}_r,\pm,\delta}$. Using the estimates on Sobolev norms supplied by Lemma 1:

$$T_{p,j}e_{\tilde{\Omega}_r}(\mathbb{Z}^n) = \mu(\tilde{\Omega}_r) + O(\delta) + p^{\beta(j,n)}O(\delta^{1/2-(n^2-1)/2-\varepsilon}).$$

Choosing δ optimally, one obtains (possibly for a new ε)

$$e_{\tilde{\Omega}_r}(\mathbb{Z}^n) = \mu(\tilde{\Omega}_r) + O(p^{2\beta(j,n)/n^2+\varepsilon}).$$

□

Note that a hyperplane $H \subset (\mathbb{Z}/p\mathbb{Z})^n$ of codimension j determines, by taking its inverse image in $\mathbb{Z}^n$, a sublattice $L_H \subset \mathbb{Z}^n$ so that $\mathbb{Z}^n/L \equiv (\mathbb{Z}/p\mathbb{Z})^j$. As H varies through all hyperplanes in $(\mathbb{Z}/p\mathbb{Z})^n$, the corresponding (rescaled) lattices $p^{-j/n}L_H$ vary through the Hecke orbit of $\mathbb{Z}^n$ under $T_{p,j}$. With this, we may translate the previous result into a statement about hyperplanes. Note that the number of hyperplanes of codimension j in $(\mathbb{Z}/p\mathbb{Z})^n$ is $p^{j(n-j)}(1+O(p^{-1}))$; utilizing this, we obtain:

Theorem 2. *Fix j and let $\Omega \subset \mathbb{R}^n$ be compact. Let $\varepsilon > 0$. For $0 \leqq r \leqq \infty$ set $c_r = \mu(\{g \in \mathrm{SL}_n(\mathbb{Z})\backslash\mathrm{SL}_n(\mathbb{R}) : |\mathbb{Z}^n g \cap \Omega| = r\})$. Assume that Ω contains a neighbourhood of the origin and is smooth w.r.t. Lebesgue measure.*

Then the number of hyperplanes of codimension j in $\mathbb{F}_p^n$ that intersect $p^{j/n}\Omega$ in precisely r points is

$$c_r p^{j(n-j)}(1 + O_{\Omega,r,\varepsilon}(p^{\frac{2\beta(j,n)}{n^2}+\varepsilon})).$$

Here $\beta(j,n)$ is as in (13).

In particular, as $p \to \infty$, a random system of j linear congruences in n variables modulo p has exactly r solutions in $p^{j/n}\Omega$ with probability c_r.

By way of comparison, let us note that Gan and Oh in [GO] use Hecke equidistribution to study points on certain varieties admitting a group action, cf. [GO, Thm 4.7]. The idea of the above theorem is similar, but in the context at hand our methods obtain considerably sharper error estimates (indeed the exponent of the above error term is about twice as good as that which would be obtained from [GO, Thm 4.7]).

4. Analysis on the space of affine lattices

In this section we set up the necessary framework to prove a version of Theorem 2 in the context of *affine* hyperplanes. The main result is the computation of the operator norm of an "affine Hecke operator"; this is done by reducing to the case of the usual Hecke operators $T_{p,j}$ on GL_n.

The reader who wishes to take the proof for granted may read only the definition of these operators at the start of Section 4.1 and proceed to Section 5.

4.1. **Hecke operators for affine lattices.** Let $\mathcal{AL}(V)$ denote the space of *affine lattices* in $\mathbb{R}^n$ of covolume V. Here an *affine lattice of covolume V* is a translate of a lattice of covolume V. These form a homogeneous space for $\mathrm{ASL}_n(\mathbb{R}) = \mathrm{SL}_n(\mathbb{R}) \ltimes \mathbb{R}^n$. If L is an affine lattice, the set $(L - L) = \{\lambda_1 - \lambda_2 : \lambda_1, \lambda_2 \in L\}$ is a *usual* lattice of the same covolume. One has a natural family of "Hecke operators": for each $1 \leqq j \leqq n-1$ we define a correspondence

$$\mathcal{AL}(V) \overset{AT_{p,j}}{\to} \mathcal{AL}(p^j V)$$

which is equivariant for the $\mathrm{ASL}_n(\mathbb{R})$-action. Namely,

$$AT_{p,j}(L) = \frac{\sum_{L' \subset L, (L-L)/(L'-L') \equiv (\mathbb{Z}/p)^j} L'}{\sum_{L'} 1}. \tag{15}$$

This associates to a lattice of covolume L a formal sum of lattices of covolume $p^j V$; in particular, it induces a map from $L^2(\mathcal{AL}(V))$ to $L^2(\mathcal{AL}(p^{-j}V))$; this map will also be denoted $AT_{p,j}$. Our aim (realized eventually in Lemma 9) is to compute its norm when restricted to the complement of the constants; it will be no worse than for the usual SL_n-Hecke operator.

Let $\mathcal{AL} = \bigcup_V \mathcal{AL}(V)$. It is a homogeneous space for $\mathrm{AGL}_n(\mathbb{R}) = \mathrm{GL}_n(\mathbb{R}) \ltimes \mathbb{R}^n$, which we shall view as acting on the right, and it possesses an invariant measure for this action (a caution: $\mathrm{AGL}_n(\mathbb{R})$ is *not unimodular* and it *has no center*). For any ring R, we consider $\mathrm{AGL}_n(R) = \{(A, \mathbf{v}) : A \in \mathrm{GL}_n(R), \mathbf{v} \in$

$R^n\}$ acting on the right on R^n via $\mathbf{x}\cdot(A,\mathbf{v}) = \mathbf{x}A+\mathbf{v}$. The multiplication rule is $(A,\mathbf{v}).(A',\mathbf{v}') = (AA', \mathbf{v}A'+\mathbf{v}')$. With this definition, it is easy to verify that the stabilizer of the affine lattice $\mathbb{Z}^n$ under the $\mathrm{AGL}_n(\mathbb{R})$-action is $\mathrm{AGL}_n(\mathbb{Z})$.

Let $\mathbb{Z}[1/p]$ denote the ring of p-integers (rational numbers whose denominators are divisible by no primes other than p), i.e. the localization of $\mathbb{Z}$ at p.

Let $\mathbb{Z}_p \subset \mathbb{Q}_p$, as usual, be the maximal compact subring of the p-adic numbers. Considering $\mathbb{Z}[1/p]$ as a subset of $\mathbb{Q}_p$, we have $\mathbb{Z}[1/p]\cap\mathbb{Z}_p = \mathbb{Z}$, $\mathbb{Z}[1/p]+\mathbb{Z}_p = \mathbb{Q}_p$ and $\mathbb{Z}_p^\times\cdot\mathbb{Z}[1/p]^\times = \mathbb{Q}_p^\times$.

$\mathrm{AGL}_n(\mathbb{Q}_p)$ acts on "affine $\mathbb{Z}_p$-lattices in $\mathbb{Q}_p^n$", i.e. translates of a free, rank n, $\mathbb{Z}_p$-submodule of $\mathbb{Q}_p^n$. Set $K_p \subset \mathrm{AGL}_n(\mathbb{Q}_p)$ to be the stabilizer of $\mathbb{Z}_p^n$ in this action. Thus $K_p = \mathrm{AGL}_n(\mathbb{Z}_p) = \{(A,\mathbf{v}) : A \in \mathrm{GL}_n(\mathbb{Z}_p), \mathbf{v}\in\mathbb{Z}_p^n\}$.

Lemma 6. *$\mathcal{AL}$ is naturally identified with* $\mathrm{AGL}_n(\mathbb{Z}[1/p])\backslash\mathrm{AGL}_n(\mathbb{R}) \times \mathrm{AGL}_n(\mathbb{Q}_p)/K_p$.

Here note that we have considered $\mathrm{AGL}_n(\mathbb{Z}[1/p])$ as a subgroup of $\mathrm{AGL}_n(\mathbb{R})\times \mathrm{AGL}_n(\mathbb{Q}_p)$ by means of the natural diagonal embedding $\mathbb{Z}[1/p]\hookrightarrow\mathbb{R}\times\mathbb{Q}_p$.

Proof. Indeed, consider the map

$$\mathrm{AGL}_n(\mathbb{Z})\backslash\mathrm{AGL}_n(\mathbb{R}) \hookrightarrow \mathrm{AGL}_n(\mathbb{Z}[1/p])\backslash\mathrm{AGL}_n(\mathbb{R}) \times \mathrm{AGL}_n(\mathbb{Q}_p)/K_p$$

which is induced from the inclusion $g\mapsto(g,1)$ of $\mathrm{AGL}_n(\mathbb{R})$ into $\mathrm{AGL}_n(\mathbb{R})\times \mathrm{AGL}_n(\mathbb{Q}_p)$.

It is an inclusion as $\mathrm{AGL}_n(\mathbb{Z}[1/p])\cap K_p = \mathrm{AGL}_n(\mathbb{Z})$. We claim it is surjective. It suffices to verify that $\mathrm{AGL}_n(\mathbb{Q}_p) = \mathrm{AGL}_n(\mathbb{Z}[1/p])\cdot K_p$.

Note first that $\det(\mathrm{GL}_n(\mathbb{Z}[1/p])\cdot\mathrm{GL}_n(\mathbb{Z}_p)) = \mathbb{Z}[1/p]^\times\cdot\mathbb{Z}_p^\times = \mathbb{Q}_p^\times$. On the other hand, $\mathrm{SL}_n(\mathbb{Z}[1/p])$ is dense in $\mathrm{SL}_n(\mathbb{Q}_p)$ (as follows from strong approximation for SL_n) and we see that $\mathrm{GL}_n(\mathbb{Z}[1/p])\cdot\mathrm{GL}_n(\mathbb{Z}_p)$ is dense in $\mathrm{GL}_n(\mathbb{Q}_p)$. This implies $\mathrm{GL}_n(\mathbb{Z}[1/p])\cdot\mathrm{GL}_n(\mathbb{Z}_p) = \mathrm{GL}_n(\mathbb{Q}_p)$ (for, given $g\in\mathrm{GL}_n(\mathbb{Q}_p)$, the coset $g\cdot\mathrm{GL}_n(\mathbb{Z}_p)$ must intersect $\mathrm{GL}_n(\mathbb{Z}[1/p])\cdot\mathrm{GL}_n(\mathbb{Z}_p)$ by the denseness just established).

Therefore the set of products

$$\{(AA',\mathbf{v}A'+\mathbf{v}') : A\in\mathrm{GL}_n(\mathbb{Z}[1/p]), A'\in\mathrm{GL}_n(\mathbb{Z}_p), \mathbf{v}\in\mathbb{Z}[1/p]^n, \mathbf{v}'\in\mathbb{Z}_p^n\}$$

projects surjectively onto the first factor. On the other hand, given $A\in \mathrm{GL}_n(\mathbb{Z}[1/p])$ and $A'\in\mathrm{GL}_n(\mathbb{Z}_p)$ the set of vectors $(\mathbf{v}A'+\mathbf{v}') = (\mathbf{v}+\mathbf{v}'A'^{-1})A'$ exhausts $\mathbb{Q}_p^n$, as $\mathbf{v}$ varies through $\mathbb{Z}[1/p]^n$ and $\mathbf{v}'$ varies through $\mathbb{Z}_p^n$. Thus $\mathrm{AGL}_n(\mathbb{Z}[1/p])\cdot K_p = \mathrm{AGL}_n(\mathbb{Q}_p)$. $\square$

This allows us to transfer questions about the action of $AT_{p,j}$ to questions about representation theory.

In fact, observe that the previous lemma ensures that any K_p-bi-invariant measure on $\mathrm{AGL}_n(\mathbb{Q}_p)$ acts on $L^2(\mathcal{AL})$. It is not hard to construct such a measure whose action on $\mathcal{AL}$ corresponds to $AT_{p,j}$ (defined in (15)). Namely, define $\mu_{AT_{p,j}}$ to be the restriction of Haar measure to

$$\{(A,\mathbf{v}) : A \in \mathrm{GL}_n(\mathbb{Z}_p)\mathrm{diag}(p^{-1},p^{-1},\dots,p^{-1},1,1,\dots,1)\mathrm{GL}_n(\mathbb{Z}_p), \mathbf{v} \in \mathbb{Z}_p^n \cdot A\}$$
$$= K_p \cdot (\mathrm{diag}(p^{-1},\dots,p^{-1},1,1,1,\dots,1),\mathbf{0}) \cdot K_p, \tag{16}$$

normalized so the total mass of $\mu_{AT_{p,j}}$ is 1. (Here there are exactly j p^{-1}s in $\mathrm{diag}(p^{-1},p^{-1},\dots,p^{-1},1,1,\dots,1)$.) In order to verify that the action of $\mu_{AT_{p,j}}$ coincides with that of $AT_{p,j}$ one notes that, since the actions of $\mu_{AT_{p,j}}$ and $AT_{p,j}$ on $L^2(\mathcal{AL})$ are $\mathrm{AGL}_n(\mathbb{R})$-equivariant, it suffices to check that they coincide when applied to $\mathbb{Z}^n$. This is easily done.

Note that the resulting measure is independent of whether one chooses a left or right Haar measure on $\mathrm{AGL}_n(\mathbb{Q}_p)$.

For each $V > 0$, we normalize the $\mathrm{ASL}_n(\mathbb{R})$-invariant measure on $\mathcal{AL}(V)$ so that the total mass is 1. We also fix any $\mathrm{AGL}_n(\mathbb{R})$-invariant measure on $\mathcal{AL}$.

Lemma 7. *Let $V > 0$. Let $L_0^2(\mathcal{AL}(V))$ denote the orthogonal complement of the constants in $L^2(\mathcal{AL}(V))$. Let $\mathcal{C} \subset L^2(\mathcal{AL})$ denote the subspace of $L^2(\mathcal{AL})$ consisting of functions that are essentially constant on each subset $\mathcal{AL}(V) \subset \mathcal{AL}$. Let $L_0^2(\mathcal{AL})$ be the orthogonal complement of $\mathcal{C}$ in $L^2(\mathcal{AL})$.*

The operator norm of $AT_{p,j}$, considered as a map $L_0^2(\mathcal{AL}(V)) \to L^2(\mathcal{AL}(p^{-j}V))$, is bounded above by the operator norm of the map $AT_{p,j}$, considered as a map $L_0^2(\mathcal{AL}) \to L^2(\mathcal{AL})$.

Proof. Fix s, a non-negative continuous compactly supported bump function on $\mathbb{R}^+$ centered around 1. For L an affine lattice, we denote by $\mathrm{vol}(L)$ the covolume of L.

For any V and any function f on $\mathcal{AL}(V)$, let F_f be the function on $\mathcal{AL}$ given by $F_f(L) = s(\frac{\mathrm{vol}(L)}{V})f(L \cdot (\frac{V}{\mathrm{vol}(L)})^{1/n})$. Then one has $||F_f||_2 = C||f||_2$ for some constant C that depends on s, V and the choice of measure on $\mathcal{AL}$. One may check also that $f \in L_0^2(\mathcal{AL}(V))$ holds if and only if $F_f \in L_0^2(\mathcal{AL})$.

On the other hand, one verifies that $AT_{p,j}F_f = F_{AT_{p,j}f}$, and one deduces the result. □

4.2. **Computation of the norm of $AT_{p,j}$ on $L_0^2(\mathcal{AL})$ for $n \geqq 3$.** In this section we apply some representation theory to compute the operator norm of $AT_{p,j} : L_0^2(\mathcal{AL}) \to L^2(\mathcal{AL})$.

We now recall the representation theory for $\mathrm{AGL}_n(\mathbb{Q}_p)$. Let N be the unipotent radical of AGL_n, so $N(\mathbb{Q}_p) = \mathbb{Q}_p^n$, and let ψ be a nonzero character of $N(\mathbb{Q}_p)$; let P_ψ be the stabilizer of ψ in $\mathrm{GL}_n(\mathbb{Q}_p)$. (Here, $\mathrm{GL}_n(\mathbb{Q}_p)$ is viewed as acting on $N(\mathbb{Q}_p)$, and therefore the character group of $N(\mathbb{Q}_p)$, by conjugation.)

Then – the Mackey theory implies – an irreducible representation of $\mathrm{AGL}_n(\mathbb{Q}_p)$ is either:

1. Lifted from an irreducible representation of $\mathrm{GL}_n(\mathbb{Q}_p)$, via the natural map $\mathrm{AGL}_n(\mathbb{Q}_p) \to \mathrm{GL}_n(\mathbb{Q}_p)$ with kernel $N(\mathbb{Q}_p)$;

(2) Induced, of the form

$$\mathrm{Ind}_{P_\psi \cdot N(\mathbb{Q}_p)}^{\mathrm{AGL}_n(\mathbb{Q}_p)}(\sigma.\psi).$$

Here σ is an irreducible representation of P_ψ, and $\sigma.\psi$ is the representation of $P_\psi \cdot N(\mathbb{Q}_p)$ that is σ when restricted to P_ψ, and is scalar multiplication by $\psi(n)$ when restricted to $N(\mathbb{Q}_p)$.

Lemma 8. *The operator norm of $\mu_{AT_{p,j}}$ (defined as in (16)) on $L^2_0(\mathcal{AL})$ is $\ll_n p^{\beta(j,n)}$.*

Proof. We give the proof for $n \geqq 3$. For $n = 2$ the result remains valid and may be proved by a direct spectral decomposition of $L^2_0(\mathcal{AL})$ (roughly speaking, "Fourier analysis along N"); since we present in subsequent sections an alternate and very direct approach to the case $n = 2$ we will not give details here.

Set $\tilde{\mathcal{AL}} = \mathrm{AGL}_n(\mathbb{Z}[1/p]) \backslash \mathrm{AGL}_n(\mathbb{R}) \times \mathrm{AGL}_n(\mathbb{Q}_p)$. Then $\mathcal{AL}$ is the quotient of $\tilde{\mathcal{AL}}$ by the compact group $\mathrm{AGL}_n(\mathbb{Z}_p)$.

Note that the right-invariant Haar measure on $\mathrm{AGL}_n(\mathbb{R}) \times \mathrm{AGL}_n(\mathbb{Q}_p)$ is invariant under *left* multiplication by $\mathrm{AGL}_n(\mathbb{Z}[1/p])$. We equip $\tilde{\mathcal{AL}}$ with the quotient measure.

There is a "determinant" map $\tilde{\mathcal{AL}} \to \mathbb{Z}[1/p]^\times \backslash \mathbb{R}^\times \times \mathbb{Q}_p^\times$. Let $L^2_0(\tilde{\mathcal{AL}})$ be the orthogonal complement in $L^2(\tilde{\mathcal{AL}})$ to functions pulled back from $\mathbb{Z}[1/p]^\times \backslash \mathbb{R}^\times \times \mathbb{Q}_p^\times$. (More precisely, take the orthogonal complement of the pullbacks of continuous, compactly supported functions.) Then one sees that, under the map $\tilde{\mathcal{AL}} \to \mathcal{AL}$, functions in $L^2_0(\mathcal{AL})$ pull back to functions in $L^2_0(\tilde{\mathcal{AL}})$.

$L^2_0(\tilde{\mathcal{AL}})$ may be decomposed as a direct integral of $\mathrm{AGL}_n(\mathbb{Q}_p)$-representations which do not involve any one-dimensional irreducible representations. This can be proved by an explicit spectral decomposition, or more abstractly as follows: suppose that the spectral support of a nonzero $F \in L^2_0(\tilde{\mathcal{AL}})$ were supported entirely on 1-dimensional representations of $\mathrm{AGL}_n(\mathbb{Q}_p)$. In particular, F is $\mathrm{ASL}_n(\mathbb{Q}_p)$-invariant. Now, convolve F with an appropriate compactly supported, continuous function in $\mathrm{AGL}_n(\mathbb{R}) \times \mathrm{AGL}_n(\mathbb{Q}_p)$; by doing this, we may replace F by $F' \neq 0$ which is continuous and also $\mathrm{ASL}_n(\mathbb{Q}_p)$-invariant. One verifies by an approximation argument (viz. $\mathrm{ASL}_n(\mathbb{Z}[1/p])$ is dense in $\mathrm{ASL}_n(\mathbb{R})$) together with the continuity of F' that F' is $\mathrm{ASL}_n(\mathbb{R})$-invariant. Thus F' is $\mathrm{ASL}_n(\mathbb{R}) \times \mathrm{ASL}_n(\mathbb{Q}_p)$ invariant; it is therefore the pullback of a function on $\mathbb{Z}[1/p]^\times \backslash \mathbb{R}^\times \times \mathbb{Q}_p^\times$. On the other hand, since $F' \in L^2_0(\tilde{\mathcal{AL}})$, F' is perpendicular to such pullbacks, so $||F'||_2^2 = 0$, which is a contradiction.

It therefore suffices to bound the operator norm of $\mu_{AT_{p,j}}$ in each of the types of representation considered above, excluding case (1) when the representation of $\mathrm{GL}_n(\mathbb{Q}_p)$ is one-dimensional.

(1) Representations lifted from $\mathrm{GL}_n(\mathbb{Q}_p)$: It is clear from the definitions – see remarks before (13) – that the operator norm of $\mu_{AT_{p,j}}$ on a representation that is lifted from an *infinite-dimensional* representation of $\mathrm{GL}_n(\mathbb{Q}_p)$ is bounded by $p^{\beta(j,n)}$. (Remark that the push-forward of the measure $\mu_{AT_{p,j}}$ to $\mathrm{GL}_n(\mathbb{Q}_p)$ is just the $\mathrm{GL}_n(\mathbb{Z}_p)$-bi-invariant measure corresponding to the *usual* Hecke operator T_j (for $\mathrm{GL}_n(\mathbb{Q}_p)$) – see (12).)

    Note this requires $n \geqq 3$!

(2) Induced representations: It is formal to see that the operator norm of $\mu_{AT_{p,j}}$ in the induced representation $\mathrm{Ind}_{P_\psi \cdot N(\mathbb{Q}_p)}^{\mathrm{AGL}_n(\mathbb{Q}_p)}(\sigma.\psi)$ is bounded by the corresponding operator norm in

$$W = \mathrm{Ind}_{P_\psi \cdot N(\mathbb{Q}_p)}^{\mathrm{AGL}_n(\mathbb{Q}_p)}(1),$$

the induction of *the trivial representation.* $N(\mathbb{Q}_p)$ acts trivially on W, so W is the extension of a certain unitary $\mathrm{GL}_n(\mathbb{Q}_p)$-representation. Further, one may check that W does not weakly contain any 1-dimensional representation of $\mathrm{GL}_n(\mathbb{Q}_p)$ – indeed, directly from the definition, one may verify that W is a direct integral of representations of $\mathrm{GL}_n(\mathbb{Q}_p)$ that are induced from the parabolic of type $(n-1, 1)$.

    One verifies as in Case (1) that the operator norm of $\mu_{AT_{p,j}}$ in this case is again bounded by $p^{\beta(j,n)}$.

We conclude that the operator norm of $\mu_{AT_{p,j}}$ on $L^2_0(\tilde{\mathcal{AL}})$ (and so also the operator norm of $AT_{p,j}$ acting on $L^2_0(\mathcal{AL})$ – see Lemma 7 for definitions) is bounded by $p^{\beta(j,n)}$. $\square$

Combining Lemma 7, the definition of $\mu_{AT_{p,j}}$ in (16), and Lemma 8, we have proved:

Lemma 9. *The operator $AT_{p,j}$, considered as a map from $L^2_0(\mathcal{AL}(V))$ to $L^2_0(\mathcal{AL}(p^{-j}V))$, has operator norm $\ll_n p^{\beta(j,n)}$.*

5. Inhomogeneous linear congruences

We fix a left-invariant Riemannian metric on $\mathrm{ASL}_n(\mathbb{R})$. For $V \in \mathbb{R}_+$, set $L_0(V) = V^{1/n} \cdot \mathbb{Z}^n$; then $g \mapsto L_0(V)g$ identifies $\mathcal{AL}(V)$ with a quotient of $\mathrm{ASL}_n(\mathbb{R})$, and we give it the induced metric. We assign $\mathcal{AL}(V)$ the measure μ that is invariant under $\mathrm{ASL}_n(\mathbb{R})$ and has total mass 1.

Set $\tilde{\Omega}_r = \{L \in \mathcal{AL}(p^j) : |L \cap \Omega p^{j/n}| = r\}$. **WARNING:** Note that the map from $\mathcal{AL}(V)$ to $\mathcal{AL}(p^j V)$ defined as "scaling by $p^{j/n}$" does *not* commute with the $\mathrm{ASL}_n(\mathbb{R})$-action.

Lemma 10. *Let $\Omega \subset \mathbb{R}^n$ be smooth w.r.t. Lebesgue measure. Then $\tilde{\Omega}_r$, considered as a subset of $\mathcal{AL}(p^j)$, is C-smooth for a constant C that is independent of p.*

Proof. We mimic the proof of Lemma 4. Let U_ε be an ε-neighbourhood of the identity in $\mathrm{ASL}_n(\mathbb{R})$, and suppose $L \in \partial_\varepsilon \tilde{\Omega}_r$. Then there exist $u, u' \in U_\varepsilon$ so that $Lu \in \tilde{\Omega}_r$ and $Lu' \notin \tilde{\Omega}_r$.

It follows that $|L \cap \Omega p^{j/n} u^{-1}| = r$ and $|L \cap \Omega p^{j/n} u'^{-1}| \neq r$. Now there is a constant C so that the symmetric difference of $\Omega p^{j/n} u^{-1}$ and $\Omega p^{j/n} u'^{-1}$ has volume $\leqq Cp^j \varepsilon$, and L contains at least one point belonging to this symmetric difference. Denote this symmetric difference by S.

Now note – by a version of Siegel's theorem for $\mathcal{AL}$ that is actually much easier, since one can integrate first over translates of a given lattice – one has $\mathrm{vol}\{L \in \mathcal{AL}(V) : |L \cap S| \geqq 1\} \leqq V^{-1} \mathrm{vol}(S)$. It follows that $\tilde{\Omega}_r$ is smooth as claimed. (Note that Ω containing a neighbourhood of the origin is not necessary for this argument.) $\square$

Let f be an C^∞ and L^1 function on $\mathcal{AL}(p^j)$, $f_0 = f - \int f$, and $k = [\frac{n^2+n-1}{2}]$, $\alpha = \frac{n^2+n-1}{2} - k$. Then, proceeding as in (14), and using Lemma 9, we see:

$$AT_{p,j} f(\mathbb{Z}^n) - \int_{\mathcal{AL}(p^j)} f \, d\mu = AT_{p,j} f_0(\mathbb{Z}^n) \ll p^{\beta(j,n)} S_k(f_0)^{1-\alpha-\varepsilon} S_{k+1}(f_0)^{\alpha+\varepsilon}.$$

We may now proceed exactly as before, applying Lemma 1 with $X = \mathcal{AL}(p^j)$. At this point it is important to note (since p is varying) that the implicit constants furnished when applying Lemma 1 to $X = \mathcal{AL}(p^j)$ do not depend on p. This is immediate from the proof of Lemma 1; indeed the implicit constant depends only on k_δ.

Theorem 3. *Fix j and let $\Omega \subset \mathbb{R}^n$ be compact and smooth w.r.t. Lebesgue measure. Let $\varepsilon > 0$. Set $c'_r = \mu\{g \in \mathrm{ASL}_n(\mathbb{Z}) \backslash \mathrm{ASL}_n(\mathbb{R}) : |\mathbb{Z}^n g \cap \Omega| = r\}$. Then the number of affine hyperplanes of codimension j in $\mathbb{F}_p^n$ that intersect $p^{j/n}\Omega$ in precisely r points is*

$$c'_r p^{j(n-j+1)}(1 + O_{\Omega,r,\varepsilon}(p^{\frac{2\beta(j,n)}{n^2+n}+\varepsilon})).$$

Here $\beta(j,n)$ is as in (13). In particular, as $p \to \infty$, the corresponding system of linear congruences has r solutions in $p^{j/n}\Omega$ with probability c'_r.

6. A stronger bound for $n = 2$

In this section we give an alternative approach in the inhomogeneous case; this yields an improved error bound for $n = 2$ and special choices of Ω. It seems that it should be possible to extend this approach to the case $n \geqq 3$, but we have not carried this out.

Let $\tilde{\Omega}_r$ be as in Section 5. The starting point of our approach here is Lemma 11 below, which allows us to (roughly speaking) "push down" the characteristic function of $\tilde{\Omega}_r$ to $\mathrm{SL}_n(\mathbb{Z}) \backslash \mathrm{SL}_n(\mathbb{R})$ and work only with the usual Hecke operators on $\mathrm{SL}_n(\mathbb{R})$. The main issue is then to get an understanding of the smoothness of the pushed-down function on $\mathrm{SL}_n(\mathbb{Z}) \setminus \mathrm{SL}_n(\mathbb{R})$; this is effected in Proposition 1 by two very explicit computations, dealing with the smoothness away from the cusp and near the cusp, respectively; both these computations use $n = 2$ and the special choices of Ω. However, up until Proposition 1 we are able to work with general n and Ω.

Let $\Gamma = \mathrm{SL}_n(\mathbb{Z})$, $G = \mathrm{SL}_n(\mathbb{R})$, $X = \Gamma \setminus G$, and let $T_{p,j}$ be as in Section 3. We fix $r \in \mathbb{Z}_{\geqq 0}$ once and for all. Given $\Omega \subset \mathbb{R}^n$ we define $f_\Omega : X \to [0,1]$ as

$$f_\Omega(\Gamma g) = \mathrm{vol}\Big(\big\{x \in (\mathbb{R}/\mathbb{Z})^n \;:\; |(\mathbb{Z}^n + x)g \cap \Omega| \leqq r\big\}\Big). \tag{17}$$

Now taking $\Omega \subset \mathbb{R}^n$ to be fixed, for each $\delta > 0$ we assume given some subsets $\Omega_{-,\delta}, \Omega_{+,\delta} \subset \mathbb{R}^n$ such that

$$\Omega_{-,\delta} \subset \Omega - \partial_\delta \Omega; \qquad \Omega \cup \partial_\delta \Omega \subset \Omega_{+,\delta}. \tag{18}$$

Lemma 11. *Fix j, let Ω and $\Omega_{\pm,\delta}$ be as above, and keep $p > \mathrm{diam}(\Omega)^{\frac{n}{n-j}}$. Let $N(p)$ be the total number of affine hyperplanes of codimension j in $\mathbb{F}_p^n$, and let $N_{\Omega,r}(p)$ be the number of such hyperplanes that intersect $p^{j/n}\Omega$ in at most r points. We then have, for $\delta = p^{-j/n}\sqrt{n}/2$:*

$$T_{p,j} f_{\Omega_{+,\delta}}(\mathbb{Z}^n) \leqq \frac{N_{\Omega,r}(p)}{N(p)} \leqq T_{p,j} f_{\Omega_{-,\delta}}(\mathbb{Z}^n). \tag{19}$$

Proof. For L a sublattice of $\mathbb{Z}^n$ and $x \in \mathbb{R}^n$ we define

$$g(x, L, \Omega) = \big|(x + L) \cap p^{j/n}\Omega\big|.$$

We then have

$$N(p) = p^j \sum_L 1; \qquad N_{\Omega,r}(p) = p^{j-n} \sum_L \sum_{x \in \{0,1,\ldots,p-1\}^n} I\big(g(x, L, \Omega) \leqq r\big),$$

where I is the indicator function, and both L-sums are taken over all sublattices $L \subset \mathbb{Z}^n$ such that $\mathbb{Z}^n/L \equiv (\mathbb{Z}/p\mathbb{Z})^j$. It follows from (18) and our choice of δ that

$$g(x + x', L, \Omega_{-,\delta}) \leqq g(x, L, \Omega) \leqq g(x + x', L, \Omega_{+,\delta})$$

for all $x \in \mathbb{R}^n$ and $x' \in [-\frac{1}{2}, \frac{1}{2}]^n$. Hence, writing $J = [-\frac{1}{2}, p - \frac{1}{2})$,

$$\begin{aligned} p^{j-n} \sum_L \int_{J^n} I\big(g(x, L, \Omega_{+,\delta}) \leqq r\big)\, dx &\leqq N_{\Omega,r}(p) \\ &\leqq p^{j-n} \sum_L \int_{J^n} I\big(g(x, L, \Omega_{-,\delta}) \leqq r\big)\, dx. \end{aligned} \tag{20}$$

Note that for each $L \subset \mathbb{Z}^n$ with $\mathbb{Z}^n/L \equiv (\mathbb{Z}/p\mathbb{Z})^j$ we have $p\mathbb{Z}^n \subset L$, and J^n contains exactly p^{n-j} points from each L-congruence class $x + L$. Hence the above integrals $\int_{J^n} \ldots dx$ may be rewritten as $p^{n-j} \int_{\mathcal{F}} \ldots dx$, where $\mathcal{F}$ is any fundamental domain for $\mathbb{R}^n$ modulo L. Also note that $p^{-j/n}L$ is unimodular, and (17) implies after scaling: $f_{\Omega_{\pm,\delta}}(p^{-j/n}L) = p^{-j} \int_{\mathcal{F}} I\big(|(L+x) \cap p^{j/n}\Omega_{\pm,\delta}| \leqq r\big)\, dx$. Hence it follows from the definition of $T_{p,j}$ that (20) is equivalent to (19). $\square$

Lemma 12. *Let $Y \subset X$ be a compact subset and let $\Omega \subset \mathbb{R}^n$ be K-smooth. Let f_Ω be as in (17). Then f_Ω is uniformly Lipshitz on Y: There is a constant $C = C(Y, K, \operatorname{diam}(\Omega)) > 0$ such that*

$$|f_\Omega(x) - f_\Omega(y)| \leqq C \cdot d(x,y), \qquad \forall x, y \in Y. \tag{21}$$

Proof. Viewing f_Ω as a function on $\mathrm{SL}_n(\mathbb{R})$, it suffices to prove that given any compact subset $Y_0 \subset \mathrm{SL}_n(\mathbb{R})$, there is some $C = C(Y_0, K, \operatorname{diam}(\Omega)) > 0$ such that $|f_\Omega(g_1) - f_\Omega(g_2)| \leqq C \cdot d(g_1, g_2)$ for all $g_1, g_2 \in Y_0$.

Let $A_{\Omega,g} = \{x \in \mathbb{R}^n \ : \ |(\mathbb{Z}^n + x)g \cap \Omega| > r\}$, so that $f_\Omega(g) = 1 - \operatorname{vol}(A_{\Omega,g}/\mathbb{Z}^n)$. For each subset $M \subset \mathbb{Z}^n$ we define

$$A_g(M) = \bigcap_{v \in M} (\Omega - vg) - \bigcup_{v \in \mathbb{Z}^n - M} (\Omega - vg).$$

Then, given g, for each $x \in \mathbb{R}^n$ there is a unique subset $M \subset \mathbb{Z}^n$ for which $xg \in A_g(M)$, and $x \in A_{\Omega,g}$ holds if and only if the corresponding set M has $|M| > r$. For each $w \in \mathbb{Z}^n$ we note that $xg \in A_g(M)$ implies $(x+w)g \in A_g(M-w)$; thus if the set corresponding to x is M then the set corresponding to $x+w$ is $M-w$. Let $\sim$ be the equivalence relation on subsets of $\mathbb{Z}^n$ defined by $M_1 \sim M_2 \iff [\exists w \in \mathbb{Z}^n : M_1 = M_2 - w]$.

Given a compact subset $Y_0 \subset \mathrm{SL}_n(\mathbb{R})$, we take $c(Y_0) > 0$ so that $|vg| \geqq c(Y_0) \cdot |v|$ for all $g \in Y_0$, $v \in \mathbb{R}^n$, and let $D = \operatorname{diam}(\Omega)/c(y_0)$. Then note that if $g \in Y_0$, then $A_g(M) \neq \emptyset$ implies $|v - w| \leqq D$ for all $v, w \in M$. Let F be the family of all subsets $M \subset \mathbb{Z}^n$ satisfying $|M| > r$ and $|v - w| \leqq D$ for all $v, w \in M$, and let F_0 be a set of representatives for $F/\sim$. Clearly F_0 is finite, and it is easy to give an upper bound for its cardinality which only depends on D. It follows from our observations that if $g \in Y_0$, then the set $\bigsqcup_{M \in F_0} A_g(M)g^{-1}$ (a disjoint union) is a fundamental domain for $A_{\Omega,g}$ modulo $\mathbb{Z}^n$, and hence since g is unimodular,

$$f_\Omega(g) = 1 - \sum_{M \in F_0} \operatorname{vol}(A_g(M)), \qquad \forall g \in Y_0.$$

Hence it suffices to prove that for each $M \in F_0$ there is a constant $C > 0$ such that $\big|\operatorname{vol}(A_{g_1}(M)) - \operatorname{vol}(A_{g_2}(M))\big| \leqq C \cdot d(g_1, g_2)$ for all $g_1, g_2 \in Y_0$. We may assume that $0 \in M$; then note that $A_g(M)$ may be expressed as a *finite* intersection,

$$A_g(M) = \bigcap_{v \in B_D} \begin{Bmatrix} \Omega - vg & \text{if } v \in M \\ \complement(\Omega - vg) & \text{if } v \notin M \end{Bmatrix},$$

where $B_D = \{v \in \mathbb{Z}^n \ : \ |v| \leqq D\}$. It follows that

$$\big|\operatorname{vol}(A_{g_1}(M)) - \operatorname{vol}(A_{g_2}(M))\big| \leqq \sum_{v \in B_D} \operatorname{vol}(\partial_a \Omega) \leqq K \cdot a \cdot \sharp B_D,$$

where $a = \sup_{v \in B_D} |v(g_1 - g_2)|$. The proof is completed by noting that $a \leqq C \cdot d(g_1, g_2)$ for some constant $C = C(Y_0, D) > 0$ and all $g_1, g_2 \in Y_0$. $\square$

We now specialize to $n = 2$, so that $X = \mathrm{SL}_2(\mathbb{Z}) \setminus \mathrm{SL}_2(\mathbb{R})$. Recall that we have fixed a basis X_1, X_2, X_3 for the Lie algebra of $\mathrm{SL}_2(\mathbb{R})$ and a left invariant metric d on $\mathrm{SL}_2(\mathbb{R})$.

Proposition 1. *Let $r \in \mathbb{Z}_{\geqq 0}$ be as fixed from start. Given any numbers $0 < A_1 < A_2$, there exist positive numbers K and $C_1, C_2, \ldots$ such that the following holds for each $A \in [A_1, A_2]$: If $\Omega \subset \mathbb{R}^2$ equals either the disk $\{(x,y) \mid x^2 + y^2 \leqq A^2\}$ or the square $\{(x,y) \mid |x|,|y| \leqq A\}$, then there exists a K-smooth closed subset $S \subset X$ of measure 0, such that $f_\Omega \in C^\infty(X - S)$ and $|Df_\Omega(x)| \leqq C_j \max(1, \delta^{\frac{3}{2}-j})$ for each monomial D in X_1, X_2, X_3 of order $j \geqq 1$ and all $0 < \delta < 1$, $x \in X - B(S, \delta)$.*

Note that combined with Lemma 12, the bounds on the derivatives obtained here are more than sufficient to make us able to later apply Lemma 3.

Proof. Let Y_0 be any fixed compact subset of $\mathrm{SL}_2(\mathbb{R})$. To start with, we will prove that the conclusion in Proposition 1 holds with X replaced by Y_0 throughout. In view of the proof of Lemma 12, it suffices to prove a corresponding statement with f_Ω replaced by the function $f_{M,B} : \mathrm{SL}_2(\mathbb{R}) \to \mathbb{R}$,

$$f_{M,B}(g) = \mathrm{Area}\left(\bigcap_{v \in B} \begin{cases} \Omega - vg & \text{if } v \in M \\ \complement(\Omega - vg) & \text{if } v \notin M \end{cases} \right),$$

where M, B are any fixed finite subsets $\emptyset \neq M \subset B \subset \mathbb{Z}^2$. We first assume that Ω is the disk $\Omega = \{(x,y) \mid x^2 + y^2 \leqq A\}$. Then let $S = S_1 \cup S_2$, where

$$S_{v_1,v_2} = \big\{ g \in \mathrm{SL}_2(\mathbb{R}) \ : \ |v_1 g - v_2 g| = 2A \big\}; \qquad S_1 = \bigcup_{v_1,v_2 \in B} S_{v_1,v_2};$$

$$S_{v_1,v_2,v_3} = \left\{ g \in \mathrm{SL}_2(\mathbb{R}) \ : \ \bigcap_{j=1}^{3} (\partial\Omega - v_j g) \neq \emptyset \right\}; \quad S_2 = \bigcup_{v_1,v_2,v_3 \in B} S_{v_1,v_2,v_3};$$

the unions being taken over all pairs v_1, v_2 and triples v_1, v_2, v_3, respectively, of *pairwise distinct* elements in B. We claim that S is of measure 0 and K-smooth as a subset of $\mathrm{SL}_2(\mathbb{R})$, where K only depends on A_1, A_2, B. To see this, it suffices to show that S_{v_1,v_2} and S_{v_1,v_2,v_3} are of measure 0 and K-smooth for any given pairwise distinct elements $v_1, v_2, v_3 \in \mathbb{Z}^n$, where now K only depends on A_1, A_2, v_1, v_2, v_3. We prove this for S_{v_1,v_2,v_3}; the case of S_{v_1,v_2} is easier. Since S_{v_1,v_2,v_3} only depends on $v_2 - v_1$ and $v_3 - v_1$, we may assume $v_1 = 0$. We may then also assume v_2, v_3 to be linearly independent, since otherwise $S_{v_1,v_2,v_3} = \emptyset$. Hence, writing $d = \det \begin{pmatrix} v_2 \\ v_3 \end{pmatrix}$, we have a diffeomorphism $\big(\mathbb{R}^+ \times \mathbb{R} \times (\mathbb{R}/2\pi\mathbb{Z})\big) \to \mathrm{SL}_2(\mathbb{R})$:

$$(a, b, \varphi) \mapsto g = \begin{pmatrix} v_2 \\ v_3 \end{pmatrix}^{-1} \begin{pmatrix} a & 0 \\ b & d/a \end{pmatrix} \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix}.$$

Note that $g \in \mathrm{SL}_2(\mathbb{R})$ satisfies $\bigcap_{j=1}^{3}(\partial\Omega - v_j g) \neq \emptyset$ if and only if the three circles in $\mathbb{R}^2$ with equal radii A and centers at $(0,0)$, $(a,0)$, $(b,d/a)$ go through a common point. One checks that this holds if and only if

$$(22) \qquad \big(a^2 b(b-a) + d^2\big)^2 = (4A^2 - a^2)d^2a^2.$$

From the geometrical description it is clear that this implies $|a|, |b| \leqq 2A$. Solving for b we obtain the equivalent equation

$$(23) \qquad (b - \frac{a}{2})^2 = \eta \frac{d}{a}\sqrt{4A^2 - a^2} - \frac{d^2}{a^2} + \frac{a^2}{4} \qquad (|a| \leqq 2A,\ \eta = \pm 1).$$

Note that for each fixed η, there are at most 8 values $a \in [-2A, 2A]$ at which the right hand side in (23) vanishes. It follows that the set of solutions $(a,b) \in \mathbb{R}^2$ to (22) is a union of four graphs of the form $\{(a, b_j(a)) : a \in I_j\}$, $j = 1,2,3,4$, where each I_j is a union of at most five closed intervals $\subset [-2A, 2A]$ and each $b_j(a)$ is a continuous function on I_j which is C^∞ in the interior of I_j. Implicit differentiation in (22) and Bézout's theorem show that there are certainly not more than 56 values of a for which $b_j'(a) = 0$ can hold; hence each I_j can be expressed as a union of at most 61 closed intervals I_{jk}, $1 \leqq k \leqq 61$ such that $b_j(a)$ is either increasing or decreasing on each interval I_{jk}. Now each curve segment $\{(a, b_j(a)) : a \in I_{jk}\}$ is easily seen to be K_1-smooth with respect to the Euclidean metric in the (a,b)-plane with $K_1 = 4 + 2|\beta_2 - \beta_1| + 2|\alpha_2 - \alpha_1|$, where (α_1, β_1) and (α_2, β_2) are the endpoints of the curve segment. Indeed, assuming $\alpha_1 < \alpha_2$ and that $b_j(a)$ is increasing on I_{jk}, one checks that for each $0 < \varepsilon \leqq 1$, the ε-neighbourhood of the given curve segment is completely contained in the region which is bounded by the two curves $\{(a - \varepsilon, b_j(a) + \varepsilon) : a \in I_{jk}\}$ and $\{(a + \varepsilon, b_j(a) - \varepsilon) : a \in I_{jk}\}$, and the four lines $a = \alpha_1 - \varepsilon$, $a = \alpha_2 + \varepsilon$, $b = \beta_1 - \varepsilon$, $b = \beta_2 + \varepsilon$; and the area of this region is $4\varepsilon^2 + 2(|\beta_2 - \beta_1| + |\alpha_2 - \alpha_1|)\varepsilon$. Using $|a|, |b| \leqq 2A$, it follows that the full set of solutions to (22) has measure 0 and is K_2-smooth in the (a,b)-plane, with $K_2 = 10^4(1 + A)$. Hence S_{v_1,v_2,v_3} is of measure 0 and K-smooth for some K which only depends on A_2, v_1, v_2, v_3, Y_0.

We now fix some $g \in Y_0 - S$. Let us write $M = \{v_1, ..., v_m\}$, $B - M = \{v_{m+1}, ..., v_b\}$, and

$$(24) \qquad F = F(w_1, ..., w_b) = \mathrm{Area}\left(\bigcap_{\ell=1}^{b} \begin{Bmatrix} \Omega - w_\ell & \text{if } \ell \leqq m \\ \complement(\Omega - w_\ell) & \text{if } \ell > m \end{Bmatrix}\right),$$

so that $f_{M,B}(g) = F(v_1 g, ..., v_b g)$. By our construction of S, there is some neighbourhood $W \subset \mathbb{R}^{2b}$ of $(v_1 g, ..., v_b g)$ such that for each $(w_1, ..., w_b) \in W$, the boundary $\mathfrak{B}$ of the region considered in (24) consists of a finite number of closed curves, each of which is a finite union of segments of the various circles $\partial\Omega - w_\ell$, joined at points $(x_1, y_1), ..., (x_K, y_K)$, say, where each (x_k, y_k) is a point of intersection between (exactly) two of the circles and varies smoothly with respect to $(w_1, ..., w_b) \in W$. But we have $F = \int_{\mathfrak{B}} x\, dy = \int_{\mathfrak{B}} (-y)\, dx$, where the integrals are taken over $\mathfrak{B}$ in positive direction. It follows that there are numbers $\eta_{k\ell} \in \{0, 1, -1\}$ such that, writing $w_\ell = (x_{w_\ell}, y_{w_\ell})$, we have $\frac{\partial}{\partial x_{w_\ell}} F = \sum_{k=1}^{K} \eta_{k\ell} y_k$ and $\frac{\partial}{\partial y_{w_\ell}} F = -\sum_{k=1}^{K} \eta_{k\ell} x_k$ throughout W.

We now wish to give bounds on derivatives of the form Dx_k and Dy_k, where D is a monomial in $\frac{\partial}{\partial x_{w_\ell}}$ and $\frac{\partial}{\partial y_{w_\ell}}$ ($\ell = 1, ..., b$) of order $j \geqq 1$. We may assume that (x_k, y_k) is a point of intersection between $\partial\Omega - w_1$ and $\partial\Omega - w_2$. The functions x_k, y_k satisfy $(x_k - x_{w_1})^2 + (y_k - y_{w_1})^2 = A^2$ and $(x_k - x_{w_2})^2 + (y_k - y_{w_2})^2 = A^2$, and applying D to these two relations we obtain

$$\begin{cases} 2(x_k - x_{w_1})Dx_k + 2(y_k - y_{w_1})Dy_k = * \\ 2(x_k - x_{w_2})Dx_k + 2(y_k - y_{w_2})Dy_k = *, \end{cases}$$

where the right hand sides are 0 or $2(x_k - x_{w_\ell})$ or $2(y_k - y_{w_\ell})$ for some ℓ if $j = 1$, while for $j \geqq 2$ they are finite sums of products of the form $[\text{const}] \cdot \prod_s D_s x_k$ or $[\text{const}] \cdot \prod_s D_s y_k$, where all D_s are monomials in $\frac{\partial}{\partial x_{w_\ell}}$ and $\frac{\partial}{\partial y_{w_\ell}}$ satisfying $1 \leqq \text{order}(D_s) < j$ and $\sum_s \text{order}(D_s) \leqq j$. (Some product may be empty, i.e. giving a constant term). Note that the determinant $\begin{vmatrix} x_k - x_{w_1} & y_k - y_{w_1} \\ x_k - x_{w_2} & y_k - y_{w_2} \end{vmatrix}$ has absolute value $|w_1 w_2| \cdot \sqrt{A^2 - |w_1 w_2|^2/4}$, where $|w_1 w_2|$ denotes the distance between w_1 and w_2. Note also that for $g \in Y_0 - B(S, \delta)$ and $(w_1, ..., w_b) = (v_1 g, ..., v_b g)$ the distance $|w_1 w_2|$ is bounded from below by a positive constant which only depends on Y_0, and $2A - |w_1 w_2| \gg \delta$. Hence $Dx_k, Dy_k \ll \delta^{\frac{1}{2} - j}$, by induction on j. It follows that for each $j \geqq 1$ there is a positive constant C_j which only depends on Y_0, M, B, A_1, A_2, j such that $|Df_{M,B}(g)| \leqq C_j \max(1, \delta^{\frac{3}{2} - j})$ for each monomial D in X_1, X_2, X_3 of order $j \geqq 1$ and all $0 < \delta < 1$, $g \in Y_0 - B(S, \delta)$.

The case of a square, $\Omega = \{(x, y) \mid |x|, |y| \leqq A\}$ is similar but easier. In this case we let $\mathfrak{S}_A = \{(x, y) \mid x \in \{0, A, -A\} \text{ or } y \in \{0, A, -A\}\}$ and

$$S = \big\{ g \in Y_0 \mid \exists v_1 \neq v_2 \in B : v_1 g - v_2 g \in \mathfrak{S}_A \big\}.$$

Then S is of measure 0 and K-smooth as a subset of $\mathrm{SL}_2(\mathbb{R})$, where K only depends on A_1, A_2, Y_0, B. Furthermore $f_{M,B} \in C^\infty(Y_0 - S)$, and this time we can give bounds on the derivatives which do not blow up: There are positive constants C_j which only depend on Y_0, M, B, A_1, A_2, j such that $|Df_{M,B}(g)| \leqq C_j$ for each monomial D in X_1, X_2, X_3 of order $j \geqq 1$ and all $g \in Y_0 - B(S, \delta)$.

It now remains to treat the case when $\Gamma g \in X$ lies far out in the cusp. We use a form of Iwasawa coordinates, writing

$$g = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix} \begin{pmatrix} \rho^{-1} & 0 \\ 0 & \rho \end{pmatrix} \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}, \qquad t \in \mathbb{R},\ \rho > 0,\ \varphi \in \mathbb{R}. \tag{25}$$

We restrict attention to the cuspidal region $X_c \subset X$ defined by $\rho < \min((4A)^{-1}, A(r + 10)^{-1})$. Writing $v_\varphi = (\cos\varphi, -\sin\varphi)$, $w_\varphi = (\sin\varphi, \cos\varphi)$, we have $g = \begin{pmatrix} \rho^{-1} v_\varphi + t\rho w_\varphi \\ \rho w_\varphi \end{pmatrix}$ and hence by (17), $f_\Omega(\Gamma g)$ is the volume of the set of those $(x,y) \in [-\frac{1}{2},\frac{1}{2}]^2$ which satisfy

$$\Big| \big\{ (n,m) \in \mathbb{Z}^2 \mid (n+x)(\rho^{-1} v_\varphi + t\rho w_\varphi) + (m+y)\rho w_\varphi \in \Omega \big\} \Big| \leqq r. \tag{26}$$

For each $x \in \mathbb{R}$ we let $\ell(x)$ be the length of the line segment $\{y \mid xv_\varphi + yw_\varphi \in \Omega\}$. Then if Ω is the disk $\{(x,y) \mid x^2+y^2 \leqq A^2\}$, we have $\operatorname{supp}(\ell) = [-A,A]$ and $\ell(x) = 2\sqrt{A^2-x^2}$ for $x \in [-A,A]$, whereas if Ω is the square $\{(x,y) \mid |x|,|y| \leqq A\}$ then for $0 < \varphi \leqq \frac{\pi}{4}$ we have $\operatorname{supp}(\ell) = [-x_1,x_1]$ with $x_1 = A\sqrt{2}\cos(\frac{\pi}{4}-\varphi)$, and

$$\ell(x) = \begin{cases} \frac{2A}{\cos\varphi} & 0 \leqq x \leqq x_2 \\ \frac{x_1 - x}{\cos\varphi \sin\varphi} & x_2 \leqq x \leqq x_1 \end{cases} \qquad (x_2 = A\sqrt{2}\cos(\tfrac{\pi}{4}+\varphi)).$$

Note also that $\ell(x)$ is even, and concave in its interval of support. It follows from our assumption on ρ that $\operatorname{supp}(\ell) \subset [-(2\rho)^{-1},(2\rho)^{-1}]$; hence only points (n,m) with $n=0$ occur in the set in (26), when $(x,y) \in [-\frac{1}{2},\frac{1}{2}]^2$. This gives

$$\begin{aligned} f_\Omega(\Gamma g) &= \int_{-1/2}^{1/2}\int_{-1/2}^{1/2} I\big(|(x\rho^{-1}v_\varphi + (\mathbb{Z}+y)\rho w_\varphi) \cap \Omega| \leqq r\big)\,dy\,dx \\ &= \int_{-(2\rho)^{-1}}^{(2\rho)^{-1}} \left\{ \begin{matrix} \rho & \text{if } \ell(x) < r\rho \\ (r+1)\rho - \ell(x) & \text{if } r\rho \leqq \ell(x) < (r+1)\rho \\ 0 & \text{if } (r+1)\rho \leqq \ell(x) \end{matrix} \right\} dx. \end{aligned}$$

Hence we obtain, in the case of the square and $0 < \varphi \leqq \frac{\pi}{4}$:

$$f_\Omega(\Gamma g) = 1 - 2A(\cos\varphi + \sin\varphi)\rho + (2r+1)\rho^2 \cos\varphi \sin\varphi.$$

Note that this formula also holds for $\varphi = 0$, and since $f_\Omega(\Gamma g)$ is invariant under $\varphi \mapsto -\varphi$ and $\varphi \mapsto \varphi + \frac{\pi}{2}$, this determines $f_\Omega(\Gamma g)$ for all values of φ. Now let S be the subset of our cuspidal region X_c defined by $\varphi \in \frac{\pi}{2}\mathbb{Z}$; we then see that $f_\Omega \in C^\infty(X_c - S)$, and a standard computation shows that S is smooth (and of measure 0) as a subset of X. Finally, if we take the basis elements X_1, X_2, X_3 to be $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, respectively, one quickly computes that in our coordinates t, ρ, φ (cf. (25)), the corresponding differential operators are

$$\begin{aligned} X_1 &= [...]\frac{\partial}{\partial t} + \rho \sin\varphi\cos\varphi \frac{\partial}{\partial\rho} - \sin^2\varphi \frac{\partial}{\partial\varphi}; \\ X_2 &= [...]\frac{\partial}{\partial t} + \rho \sin\varphi\cos\varphi \frac{\partial}{\partial\rho} + \cos^2\varphi \frac{\partial}{\partial\varphi}; \\ X_3 &= [...]\frac{\partial}{\partial t} + \rho(\sin^2\varphi - \cos^2\varphi) \frac{\partial}{\partial\rho} + 2\cos\varphi\sin\varphi \frac{\partial}{\partial\varphi}. \end{aligned}$$

Hence for each monomial D in X_1, X_2, X_3 we see that $|Df_\Omega(x)|$ is bounded on all of $X_c - S$, by some constant which only depends on A_1, A_2, D, r.

In the case of the disk we obtain $f_\Omega(\Gamma g) = 1 + 2h(\frac{r\rho}{2}) - 2h(\frac{(r+1)\rho}{2})$, where

$$h(x) = x\sqrt{A^2 - x^2} - A^2 \arctan\bigl(x^{-1}\sqrt{A^2 - x^2}\bigr).$$

Note that $h'(x) = 2\sqrt{A^2 - x^2}$. Hence in this case we may take $S = \emptyset$; we find that $f_\Omega \in C^\infty(X_c)$ and $|Df_\Omega(x)|$ is bounded on all of X_c, for each monomial D. $\square$

For Ω a disk or a square we now have the following improvement of Theorem 3. We write $\beta = \beta(1,2)$, cf. (13) above.

Theorem 4. *Fix $\varepsilon > 0$ and $A > 0$ and let $\Omega \subset \mathbb{R}^2$ be either the disk $\{(x,y) \mid x^2 + y^2 \leqq A^2\}$ or the square $\{(x,y) \mid |x|, |y| \leqq A\}$. Set $c_r' = \mu(\tilde{\Omega}_r)$ where $\tilde{\Omega}_r = \{g \in \mathrm{ASL}_2(\mathbb{Z}) \setminus \mathrm{ASL}_2(\mathbb{R}) \bigm| |\mathbb{Z}^2 g \cap \Omega| = r\}$. Then the number of affine lines in $\mathbb{F}_p^2$ that intersect $p^{1/2}\Omega$ in precisely r points is*

$$c_r' p^2 (1 + O_{A,r,\varepsilon}(p^{\frac{8\beta}{9}+\varepsilon})), \qquad \textit{as } p \to \infty.$$

Proof. Let $\widetilde{\Omega}_{\leqq r} = \cup_{s=0}^r \widetilde{\Omega}_s = \{g \in \mathrm{ASL}_2(\mathbb{R}) : |\mathbb{Z}^2 g \cap \Omega| \leqq r\}$, which we view as a subset of $\mathrm{ASL}_2(\mathbb{Z}) \setminus \mathrm{ASL}_2(\mathbb{R})$. Clearly, it suffices to prove, for each fixed $r \in \mathbb{Z}_{\geqq 0}$, that the number of affine lines in $\mathbb{F}_p^2$ that intersect $p^{1/2}\Omega$ in *at most* r points is

$$\mu(\widetilde{\Omega}_{\leqq r}) \cdot p^2 (1 + O_{A,r,\varepsilon}(p^{\frac{8\beta}{9}+\varepsilon})), \qquad \text{as } p \to \infty. \tag{27}$$

Note that we may take $\Omega_{\pm,\delta}$ in (18) as the disk or square with parameter A replaced by $A \pm \delta$. Note also that by Lemma 12 and Proposition 1, the functions $f_{\Omega_{\pm,\delta}}$ satisfy the assumptions in Lemma 3, for some constants $K, C, C_1, C_2, \ldots$ which do not depend on δ. (To extend the uniform Lipshitz bound in Lemma 12 to *all* of X we use the uniform bounds on the first derivatives of $f_{\Omega_{\pm,\delta}}$ proved in Proposition 1, together with the fact that any two points p_1, p_2 in X can be joined by a piecewise C^∞ curve of length $(1+\varepsilon)d(p_1,p_2)$ which only intersects the exceptional set S in a finite number of points. Note that this last fact is trivial in view of our explicit description of S in the proof of Proposition 1, but it actually holds for any smooth closed subset $S \subset X$ of measure 0.)

Now by the same Sobolev technique as before we find that $T_p f_{\Omega_{\pm,\delta}}(\mathbb{Z}^2) = \int_X f_{\Omega_{\pm,\delta}}\,dx + O(p^{\frac{8\beta}{9}+\varepsilon})$, uniformly for $0 < \delta < A/2$ and $p \to \infty$. But by a similar argument to that of Lemma 10, we have $\int_X f_{\Omega_{\pm,\delta}}\,dx = \mu(\widetilde{\Omega}_{\leqq r}) + O(\delta)$. Hence the estimate in (27) follows from Lemma 11, since $\delta = (2p)^{-1/2}$ and $\beta \geqq -\frac{1}{2}$. $\square$

Remark 1. It is clear that the same technique allows us to prove Theorem 4 for many other explicit regions $\Omega \subset \mathbb{R}^2$. It is an interesting problem to try to extend Proposition 1 to nice regions Ω in dimension $n \geqq 3$. Especially the treatment of the cuspidal region seems to be much more difficult for

$n \geqq 3$ than for $n = 2$. If such an extension of Proposition 1 to $n \geqq 3$ would turn out to be possible, this would lead to a corresponding improvement in Theorem 3; the error term $O(p^{\frac{2\beta}{n^2+n}+\varepsilon})$ therein could then be replaced by $O(p^{\frac{4\beta}{n^2}+\varepsilon})$.

Remark 2. By extending Lemma 3 to non-integral values of j, and using a more refined spectral analysis, it is possible improve the error term in Theorem 4 to $O(p^{\beta+\varepsilon})$.

7. Fractional Parts of Linear Forms

In this section we recall and comment on a result by Marklof [M1], concerning the number of values modulo one of a random linear form $\alpha_1 m_1 + ... + \alpha_{n-1} m_{n-1}$ at integer points $(m_1, ..., m_{n-1})$ which fall inside a given small interval. This problem may be regarded as a kind of non-discrete relative of the counting problems in $\mathbb{F}_p^n$ studied in earlier sections, and it leads to limits involving the same type of volumes in $\mathrm{SL}_n(\mathbb{Z}) \setminus \mathrm{SL}_n(\mathbb{R})$ and $\mathrm{ASL}_n(\mathbb{Z}) \setminus \mathrm{ASL}_n(\mathbb{R})$ as in Theorems 2 and 3. Hence our explicit computations in Section 8 will be of relevance also here.

We will use the following notation. Given any subset $\Omega \subset \mathbb{R}^n$ we write $\widetilde{\Omega}_r^{(\mathrm{SL})} = \{g \in \mathrm{SL}_n(\mathbb{Z}) \setminus \mathrm{SL}_n(\mathbb{R}) \mid |\mathbb{Z}^n g \cap \Omega| = r\}$ and $\widetilde{\Omega}_r^{(\mathrm{ASL})} = \{g \in \mathrm{ASL}_n(\mathbb{Z}) \setminus \mathrm{ASL}_n(\mathbb{R}) \mid |\mathbb{Z}^n g \cap \Omega| = r\}$. Also, for $a \geqq 0$ we define

$$f_r^{\mathrm{box},\mathrm{SL}_n}(a) = \mu(\widetilde{\Omega}_r^{(\mathrm{SL})}); \qquad f_r^{\mathrm{box},\mathrm{ASL}_n}(a) = \mu(\widetilde{\Omega}_r^{(\mathrm{ASL})}); \tag{28}$$

for Ω equal to the box $(-\frac{1}{2}, \frac{1}{2})^{n-1} \times (-\frac{a}{2}, \frac{a}{2}) \subset \mathbb{R}^n$ of volume a. (Note that μ denotes Haar measure on different groups in the two formulae in (28).) The proofs of Lemma 4 and Lemma 10 show that $f_r^{\mathrm{box},\mathrm{SL}_n}(a)$ and $f_r^{\mathrm{box},\mathrm{ASL}_n}(a)$ are continuous in $a > 0$, and that we may as well include part or all of the boundary of the box $(-\frac{1}{2}, \frac{1}{2})^{n-1} \times (-\frac{a}{2}, \frac{a}{2})$ in Ω. It follows from the right invariance of the Haar measure that we may take Ω to be *any* box of volume a in the definition of $f_r^{\mathrm{box},\mathrm{ASL}_n}(a)$, and *any* box of volume a centered at the origin in the definition of $f_r^{\mathrm{box},\mathrm{SL}_n}(a)$.

Theorem 5. (Marklof, [M1]**)** *Let $a > 0$, $r \in \mathbb{Z}_{\geqq 0}$, let $d_1, ..., d_{n-1} > 0$ be fixed numbers with $\prod_j d_j = 1$, and let h be a continuous probability density on $(\mathbb{R}/\mathbb{Z})^{n-1}$. For $\boldsymbol{\alpha} = (\alpha_1, ..., \alpha_{n-1}) \in (\mathbb{R}/\mathbb{Z})^{n-1}$, $N > 0$ and $\xi \in \mathbb{R}/\mathbb{Z}$, let $\mathcal{N}_a^{\boldsymbol{\alpha}}(\xi, N)$ be the number of values of integer tuples $(m_1, ..., m_{n-1})$ with $|m_j| \leqq \frac{d_j}{2} N^{1/(n-1)}$ such that $\alpha_1 m_1 + ... + \alpha_{n-1} m_{n-1} \in [\xi - \frac{a}{2N}, \xi + \frac{a}{2N}] + \mathbb{Z}$. Now take $\boldsymbol{\alpha} = (\alpha_1, ..., \alpha_{n-1})$ random according to the density function h. We then have*

$$Prob\{\mathcal{N}_a^{\boldsymbol{\alpha}}(0, N) = r\} \to f_r^{box,SL_n}(a), \qquad as\ N \to \infty. \tag{29}$$

If ξ is instead taken as a uniformly distributed random variable on $\mathbb{R}/\mathbb{Z}$, independent of $\boldsymbol{\alpha}$, then

$$\text{(30)} \qquad Prob\big\{\mathcal{N}_a^{\boldsymbol{\alpha}}(\xi,N)=r\big\} \to f_r^{box,ASL_n}(a), \qquad as \;\; N\to\infty$$

To see the relationship between Theorem 5 and Theorem 2 (with $j=1$), note that to each of the p^{n-1} tuples $\boldsymbol{\beta}=(\beta_1,...,\beta_{n-1})\in\mathbb{F}_p^{n-1}$, there corresponds a hyperplane of codimension one in $\mathbb{F}_p^n$ given by $x_n=\sum_{j=1}^{n-1}\beta_j x_j$; the number of codimension one hyperplanes which are *not* parametrized in this way is of lower order, namely $\ll p^{n-2}$. Furthermore, if $\Omega=(-\frac{1}{2},\frac{1}{2})^{n-1}\times(-\frac{a}{2},\frac{a}{2})$ and p is any large prime, then one easily checks that the $\mathbb{F}_p^n$-hyperplane $x_n=\sum_{j=1}^{n-1}\beta_j x_j$ intersects the set $p^{1/n}\Omega$ in exactly $\mathcal{N}_a^{\boldsymbol{\beta}/p}(0,p^{\frac{n-1}{n}})$ points, where $\mathcal{N}_a^{\boldsymbol{\alpha}}(\xi,N)$ is the number described in Theorem 5, with $d_1=...=d_{n-1}=1$. Hence Theorem 2 can be viewed as a discrete version of (29) for $N=p^{\frac{n-1}{n}}$, where we only consider the p^{n-1} points $\boldsymbol{\alpha}\in(p^{-1}\mathbb{Z}/\mathbb{Z})^{n-1}$ instead of *all* points $\boldsymbol{\alpha}\in(\mathbb{R}/\mathbb{Z})^{n-1}$. A similar relationship holds between Theorem 3 and (30).

Note that Theorem 5 is the same as Theorem 4.2 and Theorem 4.4 in [M1], except that we consider $|m_j|\leqq\frac{d_j}{2}N^{1/(n-1)}$ and the interval $[\xi-\frac{a}{2N},\xi+\frac{a}{2N}]+\mathbb{Z}$, instead of $1\leqq m_j\leqq d_jN^{1/(n-1)}$ and $[\xi,\xi+\frac{a}{N}]+\mathbb{Z}$; corresponding to this we take $\Omega=(-\frac{1}{2},\frac{1}{2})^{n-1}\times(\frac{a}{2},\frac{a}{2})$ in (28), and not $\Omega=(0,1]^{n-1}\times(0,a]$. (Note that (30) remains true in *both* these settings, but the limit in (29) depends on which of the two settings we consider.) The proof remains virtually the same as in [M1].

Theorem 5 generalizes a result of Mazel and Sinai, [MS], where the case $n=2$, constant h, and $a\leqq 1$ was treated, and an explicit formula was given for the limit. In Section 8 we will show how to extend these explicit formulas to *all* $a>0$ for $n=2$ and small r.

Remark 3. In principle it should be possible to prove an explicit rate of convergence in Theorem 5 by methods similar to those used in the present paper. For $n=2$ in (29), the proof in [M1] hinges on the asymptotic equidistribution of long closed horocycles in $\mathrm{SL}_2(\mathbb{Z})\setminus\mathrm{SL}_2(\mathbb{R})$, and in this case the question of the rate of convergence has been studied by a number of authors, cf. [Z, Sa1, FF, St]

Remark 4. Using a result by Shah, [Sh, Thm. 1.4], one can actually prove that any fixed, *irrational* ξ gives the same limit as random ξ in (30): For $\boldsymbol{\alpha}$ as in Theorem 5 and any fixed, irrational $\xi\in\mathbb{R}/\mathbb{Z}$, we have

$$\text{(31)} \qquad \mathrm{Prob}\big\{\mathcal{N}_a^{\boldsymbol{\alpha}}(\xi,N)=r\big\} \to f_r^{\mathrm{box,ASL}_n}(a), \qquad \text{as} \;\; N\to\infty$$

Proof of (31). We denote $G=\mathrm{SL}_n(\mathbb{R})$, $L=\mathrm{ASL}_n(\mathbb{R})$, $\Lambda=\mathrm{ASL}_n(\mathbb{Z})$, and let μ be the Haar measure on L normalized by $\mu(\Lambda\setminus L)=1$. We write $N_j=d_jN^{1/(n-1)}$, $a_N=\mathrm{diag}(N_1^{-1},N_2^{-1},...,N_{n-1}^{-1},N)\in G$, $\mathbf{v}_\xi=$

$(0,...,0,\xi) \in \mathbb{R}^n$, and $u(\boldsymbol{\alpha}) = \begin{pmatrix} 1 & & & \alpha_1 \\ & \ddots & & \vdots \\ & & 1 & \alpha_{n-1} \\ & & & 1 \end{pmatrix} \in G$ for $\boldsymbol{\alpha} = (\alpha_1,...,\alpha_{n-1}) \in \mathbb{R}^{n-1}$. Arguing as in Marklof [M1, p. 1157] and using [M1, Lemma 4.1] (cf. our Lemma 10) and standard approximation from above and below, we find that it suffices to prove that

(32)
$$\int_{\boldsymbol{\alpha}\in(\mathbb{R}/\mathbb{Z})^{n-1}} f\Big((u(\boldsymbol{\alpha})\cdot a_N, N\mathbf{v}_\xi)\Big)h(\boldsymbol{\alpha})\, d\boldsymbol{\alpha} \to \int_{\Lambda\setminus L} f(g)\, d\mu(g), \qquad \text{as } N\to\infty,$$

for each bounded continuous function $f : \Lambda \setminus L \to \mathbb{C}$. (Note: We continue to use the same conventions regarding the multiplication law in $L = \mathrm{ASL}_n(\mathbb{R})$ and the identification $\Lambda \setminus L \cong \mathcal{AL}(1)$ as in Section 4, which differ from those used in [M1].)

We now consider G as a subgroup of L via the imbedding

$$G \ni g \mapsto (1,\mathbf{v}_\xi)\cdot(g,0)\cdot(1,-\mathbf{v}_\xi) \in L.$$

It then follows from Shah, [Sh, Thm. 1.4], applied to the sequence $a_1, a_2, ...,$ that *if* $\Lambda \cdot G$ is dense in L, then

$$\lim_{N\to\infty} \int_{\boldsymbol{\alpha}\in(\mathbb{R}/\mathbb{Z})^{n-1}} f_0\Big((1,\mathbf{v}_\xi)(u(\boldsymbol{\alpha}),0)(a_N,0)(1,-\mathbf{v}_\xi)\Big)h(\boldsymbol{\alpha})\, d\boldsymbol{\alpha} = \int_{\Lambda\setminus L} f_0(g)\, d\mu(g),$$

for each bounded continuous function $f_0 : \Lambda \setminus L \to \mathbb{C}$. Taking f_0 as the right $(1,\mathbf{v}_\xi)$-shift of f, viz., $f_0(\Lambda\ell) := f\Big(\Lambda\ell\cdot(1,\mathbf{v}_\xi)\Big)$ for all $\Lambda\ell \in \Lambda\setminus L$, we obtain (32).

Hence it only remains to prove that $\Lambda\cdot G$ is dense in L. But for each fixed $g_0 \in G$, one checks by a quick computation that

$$\big\{\mathbf{w}\in\mathbb{R}^n \mid (g_0,\mathbf{w}) \in \Lambda\cdot G\big\} = M_\xi \cdot g_0 - \mathbf{v}_\xi,$$

where

$$M_\xi = \big\{\mathbf{x} + \mathbf{v}_\xi\gamma \mid \gamma \in \mathrm{SL}_n(\mathbb{Z}),\, \mathbf{x}\in\mathbb{Z}^n\big\} \subset \mathbb{R}^n.$$

Hence it suffices to prove that M_ξ is dense in $\mathbb{R}^n$. This, however, is elementary: Given $y \in \mathbb{R}^n$ and $\varepsilon > 0$ we may find integers x_j and $\gamma_{n,j}$ ($j = 1,2,...,n-1$) such that $|x_j + \gamma_{n,j}\xi - y_j| < \varepsilon$; letting $d = \gcd(\gamma_{n,1},...,\gamma_{n,n-1})$ and taking r to be any integer relatively prime to d, we may then also find integers m and x_n such that $\big|x_n + md\xi - (y_n - r\xi)\big| < \varepsilon$. Letting $\gamma_{n,n} = md + r$ and choosing integers γ_{ij} for $1 \leqq i \leqq n-1$, $1 \leqq j \leqq n$ such that $\gamma = (\gamma_{ij}) \in \mathrm{SL}_n(\mathbb{Z})$ (this is possible by [Si, Thm. 32]), we then have $|\mathbf{x} + \mathbf{v}_\xi\gamma - \mathbf{y}| < \sqrt{n}\cdot\varepsilon$. $\square$

8. Computations

We will now discuss how to compute $f_r^{\mathrm{box},\mathrm{ASL}_2}(a)$, i.e. the volume $\mu(\widetilde{\Omega}_r)$ of the set $\tilde{\Omega}_r = \{L \in \mathcal{AL}(1) : |L \cap \Omega| = r\}$, for $\Omega \subset \mathbb{R}^2$ an arbitrary rectangle of area a (cf. (28)). We will use the same basic method as in Elkies and McMullen [EM, pp. 30–37], where the case corresponding to Ω a triangle and $r = 0$ was treated.

We fix $r \in \mathbb{Z}_{\geqq 0}$, and write $f_r(a) = f_r^{\mathrm{box},\mathrm{ASL}_2}(a)$ for short. For any interval $I \subset \mathbb{R}$ we write $\Omega_I = I \times (0,1)$, so that $f_r(a) = \mu\{L : |L \cap \Omega_{(a_1,a_2)}| = r\}$ for any real numbers a_1, a_2 with $a_2 - a_1 = a$. We noted in Section 7 that $f_r(a)$ is continuous. Set $\Delta_\varepsilon F(a) = F(a+\varepsilon) - F(a)$. We wish to study the iterated difference $\Delta_{\varepsilon_1}\Delta_{\varepsilon_2} f_r(a)$ for $\varepsilon_1, \varepsilon_2 > 0$ small. We will show that for each $r \geqq 0$ there exists a continuous function $g_r(a)$ of $a > 0$ such that the following two ratios

(33)
$$(\varepsilon_1\varepsilon_2)^{-1}\mu\Big\{L : |L \cap \Omega_{(a_1,a_2)}| = r,\ |L \cap \Omega_{[a_1-\varepsilon_1,a_1]}| \geqq 1,\ |L \cap \Omega_{[a_2,a_2+\varepsilon_2]}| \geqq 1\Big\},$$
$$(\varepsilon_1\varepsilon_2)^{-1}\mu\Big\{L : |L \cap \Omega_{(a_1,a_2)}| = r,\ |L \cap \Omega_{[a_1-\varepsilon_1,a_1]}| = 1,\ |L \cap \Omega_{[a_2,a_2+\varepsilon_2]}| = 1\Big\},$$

both tend to $g_r(a)$ as $\varepsilon_1, \varepsilon_2 \to 0^+$, uniformly for a in compact subsets of $\mathbb{R}^+$. Interpreting $(\varepsilon_1\varepsilon_2)^{-1}\Delta_{\varepsilon_1}\Delta_{\varepsilon_2} f_r(a)$ in terms of such ratios, we obtain

$$\lim_{\varepsilon_1,\varepsilon_2 \to 0^+} (\varepsilon_1\varepsilon_2)^{-1}\Delta_{\varepsilon_1}\Delta_{\varepsilon_2} f_r(a) = g_r(a) - 2g_{r-1}(a) + g_{r-2}(a),$$

where we understand $g_{-1}(a) \equiv g_{-2}(a) \equiv 0$. It follows that f_r is a C^2 function satisfying

$$f_r''(a) = g_r(a) - 2g_{r-1}(a) + g_{r-2}(a). \tag{34}$$

For $m \in \mathbb{Z}^+$, $a_3 < a_4$ and $x_0, y_1, y_2 \in \mathbb{R}$, we define $g = g^{[m]}(a_3, a_4, x_0, y_1, y_2)$ to be the unique element in $\mathrm{ASL}_2(\mathbb{R})$ with $(0,0)g = (a_3, y_1)$, $(m,0)g = (a_4, y_2)$ and such that $(0,1)g$ has x-coordinate $= a_3 + (a_4 - a_3)x_0/m$. In this parametrization, the Haar measure on $\mathrm{ASL}_2(\mathbb{R})$, normalized as usual so that $\mu(\mathrm{ASL}_2(\mathbb{Z}) \setminus \mathrm{ASL}_2(\mathbb{R})) = 1$, equals

$$dg^{[m]} = \frac{6}{m^2\pi^2} dx_0\, dy_1\, dy_2\, da_3\, da_4.$$

Let S and S' denote the subsets of $\mathcal{AL}(1)$ occurring in the first and the second line of (33), respectively. Then $S' \subset S$, and for each element L in S there exists at least one $m \in \mathbb{Z}^+$ such that L has a representative in the set

$$S_0^{[m]} = \Big\{g = g^{[m]}(a_3, a_4, x_0, y_1, y_2) \;\Big|\; a_3 \in [a_1 - \varepsilon_1, a_1], a_4 \in [a_2, a_2 + \varepsilon_2],$$
$$x_0, y_1, y_2 \in [0,1), \big|\mathbb{Z}^2 g \cap \Omega_{(a_1,a_2)}\big| = r\Big\}.$$

Clearly

$$\mu(S_0^{[m]}) = \frac{6}{m^2\pi^2}\int_{a_1-\varepsilon_1}^{a_1}\int_{a_2}^{a_2+\varepsilon_2} V_r^{[m]}(a_1, a_2, a_3, a_4)\, da_3\, da_4, \tag{35}$$

where $V = V_r^{[m]}(a_1, a_2, a_3, a_4)$ is the three-dimensional Euclidean volume

(36)
$$V = \Big|\Big\{(x_0, y_1, y_2) \in (0,1)^3 \;\Big|\; \big|\mathbb{Z}^2 g^{[m]}(a_3, a_4, x_0, y_1, y_2) \cap \Omega_{(a_1,a_2)}\big| = r\Big\}\Big|.$$

Writing $V_r^{[m]}(a) := V_r^{[m]}(a_1, a_2, a_1, a_2)$ (recall $a = a_2 - a_1$), we will prove that for $a_3 \in [a_1 - \varepsilon_1, a_1]$ and $a_4 \in [a_2, a_2 + \varepsilon_2]$ we have

$$V_r^{[m]}(a_1, a_2, a_3, a_4) \to V_r^{[m]}(a) \tag{37}$$

as $\varepsilon_1, \varepsilon_2 \to 0$, uniformly for $a_2 - a_1 = a$ in any compact subset of $\mathbb{R}^+$. Hence $\lim_{\varepsilon_1,\varepsilon_2 \to 0}(\varepsilon_1\varepsilon_2)^{-1}\mu(S_0^{[m]}) = 6(m\pi)^{-2}V_r^{[m]}(a)$. We will also prove that $V_r^{[m]}(a)$ is continuous, and that if $S_1^{[m]}$ is the subset of those $g \in S_0^{[m]}$ for which $\big|\mathbb{Z}^2 g \cap \Omega_{[a_1-\varepsilon_1,a_1]}\big| \geqq 2$ or $\big|\mathbb{Z}^2 g \cap \Omega_{[a_2,a_2+\varepsilon_2]}\big| \geqq 2$, then $\mu(S_1^{[m]}) = o(\varepsilon_1\varepsilon_2)$ as $\varepsilon_1, \varepsilon_2 \to 0$, uniformly for a in compacta. Let us first note that these facts will immediately allow us to deduce our earlier claims regarding the two ratios in (33), with

$$g_r(a) = \sum_{m=1}^{r+1} \frac{6}{m^2\pi^2} V_r^{[m]}(a). \tag{38}$$

Indeed, note that if $\varepsilon_1, \varepsilon_2 < a/(r+2)$ then $S_0^{[m]} = \emptyset$ for $m > r+1$, so that $\mu(S') \leqq \mu(S) \leqq \sum_{m=1}^{r+1} \mu(S_0^{[m]})$. On the other hand, the sets $(S_0^{[m]} - S_1^{[m]})$, $m = 1, 2, ..., r+1$ are pairwise disjoint, and every element g in $\cup_m (S_0^{[m]} - S_1^{[m]})$ certainly represents a lattice in S', and is not $\mathrm{ASL}_2(\mathbb{Z})$-left equivalent to any other element in $\cup_m S_0^{[m]}$; hence $\mu(S') \geqq \sum_{m=1}^{r+1}(\mu(S_0^{[m]}) - \mu(S_1^{[m]}))$. This leads to the desired conclusion.

Hence it now only remains to prove our statements made in connection with (37). We fix J as some large integer. We keep $0 < 2a < J$, $0 < \varepsilon_1, \varepsilon_2 < a/(r+2)$, $a_2 - a_1 = a > 0$, $a_3 \in [a_1 - \varepsilon_1, a_1]$, $a_4 \in [a_2, a_2 + \varepsilon_2]$, and $m \leqq r+1$. Given $j \in \mathbb{Z}$ and any $g = g^{[m]}(a_3, a_4, x_0, y_1, y_2)$ in the set defining V we let L_j be the line $\{(t, j)g \mid t \in \mathbb{R}\}$. Using the definition of g one checks that the equation of L_j is

$$y = \frac{1}{a_4 - a_3}(jm + (y_2 - y_1)(x - a_3)) + y_1. \tag{39}$$

From this it follows easily that $L_j \cap \Omega_{(a_3,a_4)} = \emptyset$ whenever $|j| > 2a$; hence only lines L_j with $|j| \leqq J$ can have any points inside $\Omega_{(a_3,a_4)}$.

Define $(x(k,j), y(k,j)) = (k,j)g \in \mathbb{Z}^2 \cap L_j$. Then

$$\begin{aligned} x(k,j) &= a_3 + \frac{(jx_0 + k)(a_4 - a_3)}{m}; \\ y(k,j) &= \frac{jm}{a_4 - a_3} + \frac{(y_2 - y_1)(jx_0 + k)}{m} + y_1. \end{aligned} \tag{40}$$

In particular, because of our restriction on $\varepsilon_1, \varepsilon_2$, we have $x(k,0) \in (a_1, a_2)$ for $1 \leqq k < m$, and $x(0,0) = a_3$, $x(0,m) = a_4$, while $x(k,0) \notin [a_1 - \varepsilon_1, a_2 + \varepsilon_2]$ whenever $k < 0$ or $k > m$. By (40),

$$a_3 \leqq x(k,j) \leqq a_4 \Longleftrightarrow -jx_0 \leqq k \leqq m - jx_0. \tag{41}$$

In particular, $|j| \leqq J$ and $a_3 \leqq x(k,j) \leqq a_4$ forces $-J \leqq k \leqq m + J$. For each such pair j,k, the locus of those $x_0 \in (0,1)$ for which $x(k,j) \in [a_1 - \varepsilon_1, a_1] \cup [a_2, a_2 + \varepsilon_2]$ is a set (a union of at most two intervals) of measure $\leqq m(\varepsilon_1 + \varepsilon_2)(|j|(a_4 - a_3))^{-1} \leqq (m/a)(\varepsilon_1 + \varepsilon_2)$. Let $\mathfrak{S} \in (0,1)$ be the union of these sets taken over all $1 \leqq |j| \leqq J$ and $-J \leqq k \leqq m+J$. Then, by construction, the symmetric difference between the set in (36) defining $V_r^{[m]}(a_1, a_2, a_3, a_4)$ and the set defining $V_r^{[m]}(a_3, a_4, a_3, a_4) = V_r^{[m]}(a_4 - a_3)$ contains only points $(x_0, y_1, y_2) \in (0,1)^3$ with $x_0 \in \mathfrak{S}$. Hence

$$\left| V_r^{[m]}(a_1, a_2, a_3, a_4) - V_r^{[m]}(a_4 - a_3) \right| \leqq \left|\mathfrak{S}\right| \leqq \frac{2J(2J+m+1)m}{a}(\varepsilon_1 + \varepsilon_2).$$

Here $a \leqq a_4 - a_3 \leqq a + \varepsilon_1 + \varepsilon_2$. Hence (37) will be proved once we have proved that $V_r^{[m]}(a)$ is continuous. Similarly we obtain $\mu(S_1^{[m]}) = o(\varepsilon_1 \varepsilon_2)$ as $\varepsilon_1, \varepsilon_2 \to 0$, by writing $S_1^{[m]}$ as an integral analogous to (35), (36), and noticing that this will only involve points $(x_0, y_1, y_2) \in (0,1)^3$ with $x_0 \in \mathfrak{S}$.

It now only remains to prove that $V_r^{[m]}(a)$ is continuous. At the same time we will indicate how this volume can be calculated explicitly. Thus from now on we keep $a_3 = a_1$, $a_4 = a_2$. Note that in this case the set in (36) is symmetric under $(x_0, y_1, y_2) \longleftrightarrow (x_0, 1 - y_1, 1 - y_2)$. It follows from our observations above that we may decompose the set in (36) as follows. For each sequence $\mathbf{e} = \{e_j\}_{|j| \leq J}$ of integers satisfying $0 \leqq e_j \leqq m$, $e_0 = m - 1$ and $\sum_j e_j = r$, we define

$$\begin{aligned} W^{[m,\mathbf{e}]} &= W^{[m,\mathbf{e}]}(a) \\ &= \left\{ (x_0, y_1, y_2) \in (0,1)^3 \;\middle|\; y_1 < y_2 \text{ and } \left|\mathbb{Z}^2 g \cap \Omega_{(a_3,a_4)} \cap L_j\right| = e_j, \, \forall j \right\}. \end{aligned}$$

(Note that the condition for $j = 0$ is fulfilled for *all* $(x_0, y_1, y_2) \in (0,1)^3$, because of $e_0 = m - 1$ and our observations above.) Furthermore, for any interval $I \subset [0,1]$ we define

$$W_I^{[m,\mathbf{e}]}(a) = \left\{ (x_0, y_1, y_2) \in W^{[m,\mathbf{e}]}(a) \;\middle|\; x_0 \in I \right\}.$$

We let $I_1, I_2, ..., I_N$ be the consecutive open intervals in a Farey dissection of $[0,1]$ of order J, viz., $I_1, I_2, ..., I_N$ are the connected components which remain after all the Farey fractions $\{q_1/q_2 \mid 0 \leqq q_1 < q_2 \leqq J, \, (q_1, q_2) = 1\}$ have been removed from $[0,1)$. Then $V_r^{[m]}(a)$ can be expressed as a finite sum,

$$V_r^{[m]}(a) = 2 \sum_{\mathbf{e}} \sum_{n=1}^{N} \left| W_{I_n}^{[m,\mathbf{e}]}(a) \right|, \tag{42}$$

where $\mathbf{e}$ runs through all sequences as above. Hence it now suffices to prove that $\left|W_{I_n}^{[m,\mathbf{e}]}(a)\right|$ is continuous for all $\mathbf{e}, n$.

The point of using the Farey dissection is to ensure that if $(x_0, y_1, y_2) \in W_{I_n}^{[m,\mathbf{e}]}(a)$ then for each j with $1 \leqq |j| \leqq J$, the number jx_0 falls strictly between two consecutive integers which only depend on n and j. Hence, in view of (41), there is an integer $K = K(n, j)$ such that $a_1 < x(k, j) < a_2$ holds if and only if $k \in \{K, K+1, ..., K+m-1\}$. Furthermore, each line L_j has positive slope, since we require $y_1 < y_2$. Hence if $1 \leqq j \leqq J$ and $1 \leqq e_j \leqq m-1$, the condition $|\mathbb{Z}^2 g \cap \Omega_{(a_1,a_2)} \cap L_j| = e_j$ can be reformulated as $y(K+e_j-1, j) < 1$, $y(K+e_j, j) \geqq 1$. If $1 \leqq j \leqq J$ and $e_j = 0$ (or $e_j = m$), then the corresponding reformulation is $y(K, j) \geqq 1$ (or $y(K+m-1, j) < 1$, respectively). Similarly, if $-J \leqq j \leqq -1$, then $|\mathbb{Z}^2 g \cap \Omega_{(a_1,a_2)} \cap L_j| = e_j$ can be formulated as one or both of the inequalities $y(K+m-e_j, j) > 0$, $y(K+m-e_j-1, j) \leqq 0$.

Let us now substitute

$$y_3 = y_2 - y_1 \quad \text{and} \quad y_4 = m/a + y_3 x_0/m.$$

Then note that $y(k, j) = y_1 + (k/m)y_3 + jy_4$, a linear expression in y_1, y_3, y_4. Also note that the inequalities $0 < y_1 < y_2 < 1$ are equivalent to $0 < y_1$, $0 < y_3$, $y_1 + y_3 < 1$. In conclusion, for any given admissible $m, \mathbf{e}, n$, we can construct a finite set of linear inequalities in y_1, y_3, y_4 (the coeffients of which only depend on $m, \mathbf{e}, n$) such that if $C_{m,\mathbf{e},n}$ denotes the corresponding convex region in the (y_1, y_3, y_4)-space, then for all $(x_0, y_1, y_2) \in \mathbb{R}^3$ we have

$$(x_0, y_1, y_2) \in W_{I_n}^{[m,\mathbf{e}]}(a) \quad \Longleftrightarrow \quad x_0 \in I_n,\ (y_1, y_3, y_4) \in C_{m,\mathbf{e},n}.$$

(The region $C_{m,\mathbf{e},n}$ may well be empty. In general, it contains part but not all of its boundary $\partial C_{m,\mathbf{e},n}$.) Hence, since $dy_1 dy_2 = dy_1 dy_3$,

$$\left|W_{I_n}^{[m,\mathbf{e}]}(a)\right| = \int_{x_0 \in I_n} A_{m,\mathbf{e},n}(x_0, a)\, dx_0, \tag{43}$$

where $A_{m,\mathbf{e},n}(x_0, a)$ is the area of the projection onto the y_1, y_3-plane of the intersection between $C_{m,\mathbf{e},n}$ and the plane $y_4 = m/a + y_3 x_0/m$.

Since $C_{m,\mathbf{e},n}$ is defined by a finite set of linear inequalities, there is at most a finite subset $F \subset I_n$ of x_0-values for which the plane $y_4 = m/a + y_3 x_0/m$ is parallel to a bounding 2-simplex of $C_{m,\mathbf{e},n}$. Clearly $A_{m,\mathbf{e},n}(x_0, a)$ is continuous for $(x_0, a) \in (I_n - F) \times (0, \frac{1}{2}J)$. Note also that $0 \leqq A_{m,\mathbf{e},n}(x_0, a) \leqq \frac{1}{2}$ everywhere, since $C_{m,\mathbf{e},n}$ is restricted by $0 < y_1$, $0 < y_3$, $y_1 + y_3 < 1$. Hence (43) implies that $\left|W_{I_n}^{[m,\mathbf{e}]}(a)\right|$ is a continuous function of a, as claimed. Note that it is also clear from the above how to compute $f_r''(a)$ explicitly, at least in principle.

For a sufficiently small there is a simple explicit formula for $f_r(a)$:

Proposition 2. *We have*

$$f_r(a) = \begin{cases} \frac{3}{\pi^2}a^2 - a + 1 & \text{if } r = 0 \\ -\frac{21}{4\pi^2}a^2 + a & \text{if } r = 1 \\ \frac{3}{\pi^2}\left((r-1)^{-2} - 2r^{-2} + (r+1)^{-2}\right)a^2 & \text{if } r \geqq 2 \end{cases} \qquad \text{for } 0 < a \leqq 1.$$

If $r \geqq 5$, the formula $f_r(a) = \frac{3}{\pi^2}\left((r-1)^{-2} - 2r^{-2} + (r+1)^{-2}\right)a^2$ actually holds for all $0 < a \leqq \left[\frac{r-1}{2}\right]$.

In view of our remarks in Section 7, the case $0 < a \leqq 1$ of the above proposition can be viewed as a rederivation of the formulae proved by Mazel and Sinai in [MS]. The fact that the same formula also holds for larger values of a when $r \geqq 5$ seems to be new.

Proof. We will show that

$$g_r(a) = \frac{6}{\pi^2}(r+1)^{-2} \qquad \text{for all } 0 < a < \max\left(1, \left[\frac{r+1}{2}\right]\right). \tag{44}$$

Clearly this suffices to prove the proposition, using (34) and the fact that $\lim_{a\to 0^+} f_r(a)$ and $\lim_{a\to 0^+} f_r'(a)$ can be computed easily.

Now fix r, a as in (44), and let J be an integer $> 2a$ as before. Let $\mathbf{e} = \{e_j\}_{|j|\leqq J}$ be any sequence of integers satisfying $0 \leqq e_j \leqq e_0 + 1$ and $\sum_j e_j = r$, and write $m = e_0 + 1$ (thus $1 \leqq m \leqq r+1$). We will prove that $W^{[m,\mathbf{e}]}(a) = \emptyset$ *except* if $e_0 = r$ and $e_j = 0$ for all $j \neq 0$, and that for this exceptional sequence $\mathbf{e}$ we have $W^{[m,\mathbf{e}]}(a) = \{(x_0, y_1, y_2) \in (0,1)^3 : y_1 < y_2\}$. Since this set has volume $\frac{1}{2}$, we obtain (44) via (38) and (42).

If $m \geqq a$ then (39) implies $L_j \cap \Omega_{(a_3,a_4)} = \emptyset$ for all $j \neq 0$, and the desired conclusion follows directly from the definition of $V_r^{[m]}(a)$ and $W^{[m,\mathbf{e}]}(a)$. In particular, the proof is completed for the case $0 < a < 1$.

Now assume $1 \leqq m < a$. Note that we then have $r \geqq 3$ and $m < a < r$, by (44). We have to prove $W^{[m,\mathbf{e}]}(a) = \emptyset$; we will do this by assuming $W^{[m,\mathbf{e}]}(a)$ to contain an element (x_0, y_1, y_2), and showing that this leads to a contradiction.

Let $N = [a/m] \geqq 1$. Then note that by (39) we have $L_j \cap \Omega_{(a_3,a_4)} = \emptyset$ for all $|j| > N$, and hence $e_j = 0$ for all these j. Furthermore, for each $j \in \{1, 2, ..., N\}$ we note that if $e_j \geqq 1$ then it follows from $(x_0, y_1, y_2) \in W^{[m,\mathbf{e}]}(a)$ and (39), (40) that $jm/a + (y_2 - y_1)(e_j - 1)/m + y_1 < 1$, since the line L_j has positive slope $(y_2 - y_1)/a$. Similarly, if $e_{j-N-1} \geqq 1$ we find $(j - N - 1)m/a + (y_2 - y_1)(m + 1 - e_{j-N-1})/m + y_1 > 0$. By considering the difference between these two inequalities and using $(N+1)m/a > 1$ we obtain $e_j + e_{j-N-1} \leqq m + 1$. Note that this holds even if e_j or e_{j-N-1} is 0, since $e_j, e_{j-N-1} \leqq m$. Hence

$$r = \sum_j e_j = e_0 + \sum_{j=1}^{N}(e_j + e_{j-N-1}) \leqq m - 1 + N(m+1).$$

But $N \leqq a/m < [\frac{r+1}{2}]/m$ and hence $N \leqq ([\frac{r+1}{2}] - 1)/m = m^{-1}[\frac{r-1}{2}]$. Note here that $1 \leqq m \leqq [\frac{r-1}{2}]$. Using these facts we obtain

$$r \leqq m + m^{-1} \left[\frac{r-1}{2}\right] - 1 + \left[\frac{r-1}{2}\right] \leqq 2\left[\frac{r-1}{2}\right] \leqq r - 1.$$

This is a contradiction. □

The evaluation of $f_r(a)$ for larger values of a is much more involved. We have written a Maple program to evaluate $f_r(a)$ for small values of r, using the formulae (34), (38), (42), (43). To present the result, it is convenient to define $\Xi(a)$ for $a > 0$ by

$$\Xi''(a) = (1 - a^{-1})^2 \log|1 - a^{-1}|; \qquad \Xi(1) = \Xi'(1) = 0.$$

Then $\Xi \in C^3(\mathbb{R}^+)$, but the fourth derivative of Ξ has a logarithmic singularity at $a = 1$. Now

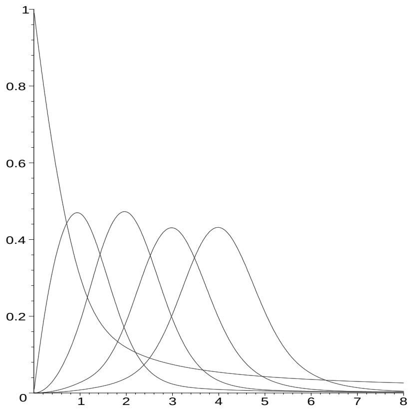
$$f_0^{\text{box},\text{ASL}_2}(a) = f_0(a) = \begin{cases} \frac{3}{\pi^2}a^2 - a + 1 & \text{if } 0 \leqq a \leqq 1 \\ \frac{12}{\pi^2}(\Xi(a) - \Xi(\frac{a}{2})) + \frac{6}{\pi^2}a\log a + c_1 a + c_2 & \text{if } 1 \leqq a, \end{cases}$$

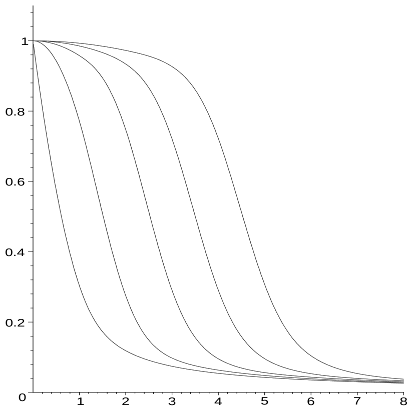
where $c_1 = \frac{6+6\log 2}{\pi^2} - 2$ and $c_2 = \frac{18\log 2}{\pi^2}$; furthermore

$$f_1(a) = \begin{cases} -\frac{21}{4\pi^2}a^2 + a & \text{if } 0 \leqq a \leqq 1 \\ -\frac{12}{\pi^2}\big(3\,\Xi(a) - 4\,\Xi(\frac{a}{2})\big) + \ell_1(a) & \text{if } 1 \leqq a \leqq 2 \\ -\frac{12}{\pi^2}\big(3\,\Xi(a) - 10\,\Xi(\frac{a}{2}) + 6\,\Xi(\frac{a}{3}) + 2\,\Xi(\frac{a}{4})\big) + \ell_2(a) & \text{if } 2 \leqq a \leqq 4 \\ -\frac{12}{\pi^2}\big(3\,\Xi(a) - 6\,\Xi(\frac{a}{2}) + 3\,\Xi(\frac{a}{3})\big) + \ell_3(a) & \text{if } 4 \leqq a; \end{cases}$$

$$f_2(a) = \begin{cases} \frac{11}{6\pi^2}a^2 & 0 \leqq a \leqq 1 \\ \frac{12}{\pi^2}\big(3\,\Xi(a) - 6\,\Xi(\frac{a}{2})\big) + \ell_4(a) & 1 \leqq a \leqq 2 \\ \frac{12}{\pi^2}\big(3\,\Xi(a) - 24\,\Xi(\frac{a}{2}) + 24\,\Xi(\frac{a}{3}) + 4\,\Xi(\frac{a}{4})\big) + \ell_5(a) & 2 \leqq a \leqq 3 \\ \frac{12}{\pi^2}\big(3\,\Xi(a) - 20\,\Xi(\frac{a}{2}) + 36\,\Xi(\frac{a}{3}) - 12\,\Xi(\frac{a}{4}) - 6\,\Xi(\frac{a}{6})\big) + \ell_6(a) & 3 \leqq a \leqq 4 \\ \frac{12}{\pi^2}\big(3\,\Xi(a) - 8\,\Xi(\frac{a}{2}) + 27\,\Xi(\frac{a}{3}) - 20\,\Xi(\frac{a}{4}) - 6\,\Xi(\frac{a}{6})\big) + \ell_7(a) & 4 \leqq a \leqq 9/2 \\ \frac{12}{\pi^2}\big(3\,\Xi(a) - 8\,\Xi(\frac{a}{2}) + 21\,\Xi(\frac{a}{3}) - 18\,\Xi(\frac{a}{4})\big) + \ell_8(a) & 9/2 \leqq a \leqq 6 \\ \frac{12}{\pi^2}\big(3\,\Xi(a) - 12\,\Xi(\frac{a}{2}) + 15\,\Xi(\frac{a}{3}) - 6\,\Xi(\frac{a}{4})\big) + \ell_9(a) & 6 \leqq a; \end{cases}$$

where $\ell_1(a), ..., \ell_9(a)$ are expressions of the form $d_1 \log^2 a + d_2 a \log a + d_3 \log a + d_4 a^2 + d_5 a + d_6$, with explicit constants d_j. The formulae grow quickly more complicated as r increases. We have posted a Maple file on the web containing the exact formulae for $f_r(a)$, $r = 0, 1, 2, 3, 4$, cf. [StV].





The graphs of $f_r(a)$ for $r = 0, 1, 2, 3, 4$, and their cumulative sums $\sum_{r=0}^{n} f_r(a)$.

The derivation of the precise formulae in [StV] involved heavy use of computer algebra applied on long and complicated expressions, and it is only reasonable to ask what type of tests were implemented to ascertain the correctness of the results. We consider the numerical data presented in Section 9 to be our strongest evidence in this regard. As further evidence we mention that we verified $\lim_{a\to\infty} f_r(a) = 0$ for $r = 0, 1, 2, 3, 4$ by exact computation; note that this relation is far from "built-in" to our computations, as $f_r(a)$ is obtained by integration of (34) starting from $a = 0$.

One more test is provided by considering the second moment of the random variable X_a given by $\mathrm{Prob}\{X_a = r\} = f_r(a)$ for $r = 0, 1, 2, \ldots$ (i.e., X_a is the number of points in the intersection $L \cap \Omega$ of a random translated lattice L and the box $\Omega = (0,1) \times (0,a)$). By a computation using Siegel's theorem for $\mathrm{SL}_n(\mathbb{Z}) \backslash \mathrm{SL}_n(\mathbb{R})$, one can show that for any compact set $\Omega \subset \mathbb{R}^n$ one has $\sum_{r=0}^{\infty} r^2 \cdot \mu(\widetilde{\Omega}_r^{(\mathrm{ASL})}) = \mathrm{vol}(\Omega)^2 + \mathrm{vol}(\Omega)$. Hence in particular, $E(X_a^2) = \sum_{r=0}^{\infty} r^2 \cdot f_r(a) = a^2 + a$ for all $a > 0$. This is of course easy to check by a direct computation for $0 < a \leqq 1$ in view of Proposition 2, but since $f_r(a) = \frac{3}{\pi^2}((r-1)^{-2} - 2r^{-2} + (r+1)^{-2})\, a^2$ also holds for $1 \leqq a \leqq 2$ whenever $r \geqq 5$ one obtains the non-trivial relation

$$\sum_{r=1}^{4} r^2 f_r(a) = \frac{6929}{1200\pi^2}\, a^2 + a, \qquad \text{for } 1 \leqq a \leqq 2.$$

We have verified this to hold for our explicit formulae for $f_r(a)$.

Regarding other moments, note that $\sum_{r=0}^{\infty} r \cdot f_r(a) = E(X_a) = a$ by the $\mathrm{ASL}_n(\mathbb{R})$-version of Siegel's theorem; but this formula is also a trivial consequence of (34) (which implies $\frac{d^2}{da^2} E(X_a) = 0$) and Proposition 2, and hence does not give an independent test of our formulae. Note also that all higher moments are infinite; $E(X_a^n) = \infty$ for $n \geqq 3$, by Proposition 2.

Using methods similar to those described above, we have also computed explicit formulas for $f_r^{\mathrm{box},\mathrm{SL}_2}(a)$, cf. (28). The details of these computations are slightly less involved than for $f_r^{\mathrm{box},\mathrm{ASL}_2}(a)$, since we may there proceed by studying $\frac{d}{da} f_r^{\mathrm{box,SL}_2}(a)$, i.e. the first derivative instead of the second. Note that by symmetry in the origin, $f_{2r}^{\mathrm{box,SL}_2}(a) = 0$ for all $r \geqq 0$. Note also that $f_{2r+1}^{\mathrm{box,SL}_2}(a) = 0$ whenever $a \geqq 4(r+1)$, by an easy generalization of Minkowski's theorem [Si, Thm. 10]. Our results are as follows.

Proposition 3. *We have for all $r \in \mathbb{Z}_{\geqq 0}$ and $0 < a \leqq 2$:*

$$f_{2r+1}^{box,SL_2}(a) = \begin{cases} 1 - \frac{3}{\pi^2} a & \text{if } r = 0 \\ \frac{3}{\pi^2}\left(r^{-2} - (r+1)^{-2}\right) a & \text{if } r \geqq 1. \end{cases}$$

If $r \geqq 3$, the formula $f_{2r+1}^{box,SL_2}(a) = \frac{3}{\pi^2}\left(r^{-2} - (r+1)^{-2}\right) a$ actually holds for all $0 < a \leqq 2\left[\frac{r-1}{2}\right] + 2$.

We define $\Psi(a)$ for $a > 0$ by

$$\Psi'(a) = (a^{-1} - 1)\log\left|a^{-1} - 1\right|; \qquad \Psi(1) = 0.$$

Now

$$f_1^{\mathrm{box,SL}_2}(a) = \begin{cases} 1 - \frac{3}{\pi^2} a & \text{if } 0 \leqq a \leqq 2 \\ \frac{12}{\pi^2}\left(\Psi(\frac{a}{4}) - \log a\right) + \frac{3}{\pi^2} a + \frac{12}{\pi^2}(2\log 2 - 1) & \text{if } 2 \leqq a \leqq 4 \\ 0 & \text{if } 4 \leqq a, \end{cases}$$

$$f_3^{\mathrm{box,SL}_2}(a) = \begin{cases} \frac{9}{4\pi^2} a & 0 \leqq a \leqq 2 \\ -\frac{24}{\pi^2}\Psi(\frac{a}{4}) + q_1(a) & 2 \leqq a \leqq 4 \\ \frac{12}{\pi^2}\left(\Psi(\frac{a}{4}) + 2\,\Psi(\frac{a}{8})\right) + q_2(a) & 4 \leqq a \leqq 16/3 \\ \frac{24}{\pi^2}\Psi(\frac{a}{4}) + q_3(a) & 16/3 \leqq a \leqq 8 \\ 0 & 8 \leqq a, \end{cases}$$

$$f_5^{\mathrm{box,SL}_2}(a) = \begin{cases} \frac{5}{12\pi^2} a & 0 \leqq a \leqq 2 \\ \frac{12}{\pi^2}\,\Psi(\frac{a}{4}) + q_4(a) & 2 \leqq a \leqq 4 \\ -\frac{12}{\pi^2}\left(2\,\Psi(\frac{a}{4}) + 3\,\Psi(\frac{a}{8})\right) + q_5(a) & 4 \leqq a \leqq 16/3 \\ -\frac{12}{\pi^2}\left(5\,\Psi(\frac{a}{4}) - 3\,\Psi(\frac{a}{8})\right) + q_6(a) & 16/3 \leqq a \leqq 6 \\ -\frac{12}{\pi^2}\left(5\,\Psi(\frac{a}{4}) - 3\,\Psi(\frac{a}{8}) - 2\,\Psi(\frac{a}{12})\right) + q_7(a) & 6 \leqq a \leqq 36/5 \\ -\frac{12}{\pi^2}\left(4\,\Psi(\frac{a}{4}) - 3\,\Psi(\frac{a}{8})\right) + q_8(a) & 36/5 \leqq a \leqq 8 \\ \frac{24}{\pi^2}\,\Psi(\frac{a}{4}) + q_9(a) & 8 \leqq a \leqq 12 \\ 0 & 12 \leqq a, \end{cases}$$

where $q_1(a), ..., q_9(a)$ are expressions of the form $d_1 \log a + d_2 a + d_3$, with explicit constants d_j. We refer again to [StV] for the exact formulae for $f_r^{\mathrm{box,SL}_2}(a)$, $r = 3, 5, 7, 9$.

Regarding moments, note that $\sum_{r=0}^{\infty} r \cdot f_r^{\mathrm{box},\mathrm{SL}_2}(a) = a+1$ by Siegel's theorem, and $\sum_{r=0}^{\infty} r^n \cdot f_r^{\mathrm{box},\mathrm{SL}_2}(a) = \infty$ for all $n \geqq 2$ (and all $a > 0$), by Proposition 3.

9. Numerical experiments

In this section we present some data from numerical experiments related to several of the main results in this paper.

Table 1 concerns the error term in Theorem 2 for Ω a two dimensional square, $\Omega = \Omega_a = [-\frac{\sqrt{a}}{2}, \frac{\sqrt{a}}{2}]^2 \subset \mathbb{R}^2$. We let $N_{a,r}(p)$ denote the number of lines through the origin in $\mathbb{F}_p^2$ which intersect $p^{1/2}\Omega_a$ in exactly r points. Recall the definition of $f_r^{\mathrm{box},\mathrm{SL}_2}(a)$ in (28). We note that both $N_{a,r}(p) = 0$ and $f_r^{\mathrm{box},\mathrm{SL}_2}(a) = 0$ hold whenever r is even, and also for all $a \geqq 2r+2$ (the fact that $N_{a,r}(p) = 0$ for all $a \geqq 2r+2$ follows by an easy extension of Thue's theorem, [N, Thm. 75]). We have computed the deviations

$$\left| \frac{N_{a,r}(p)}{p+1} - f_r^{\mathrm{box},\mathrm{SL}_2}(a) \right|, \qquad a \in \{0.2, 0.4, 0.6, ...\},\ a < 2r+2,$$

for $r \in \{1,3,5,7,9\}$ and certain values of p. The exact value of $f_r^{\mathrm{box},\mathrm{SL}_2}(a)$ was computed using the explicit formalae in [StV]. In Table 1 we list the maximum $\delta_r^{(\mathrm{max})}$ and the average $\delta_r^{(\mathrm{av.})}$ of these deviations.

Table 2 gives similar data concerning the error term in Theorem 4 (cf. also Remark 2): We list the maximum $\delta_r^{(\mathrm{max})}$ and the average $\delta_r^{(\mathrm{av.})}$ the deviations

$$\left| \frac{\tilde{N}_{a,r}(p)}{p(p+1)} - f_r^{\mathrm{box},\mathrm{ASL}_2}(a) \right|, \qquad a \in \{0.1, 0.2, 0.3, ..., 15.0\},$$

where $\tilde{N}_{a,r}(p)$ is the number of affine lines in $\mathbb{F}_p^2$ which intersect the square $p^{1/2}\Omega_a$ in exactly r points.

	$\delta_1^{(\mathrm{max})}$ $\delta_1^{(\mathrm{av.})}$	$\delta_3^{(\mathrm{max})}$ $\delta_3^{(\mathrm{av.})}$	$\delta_5^{(\mathrm{max})}$ $\delta_5^{(\mathrm{av.})}$	$\delta_7^{(\mathrm{max})}$ $\delta_7^{(\mathrm{av.})}$	$\delta_9^{(\mathrm{max})}$ $\delta_9^{(\mathrm{av.})}$
p=5003	$1.2 \cdot 10^{-2}$ $5.9 \cdot 10^{-3}$	$1.9 \cdot 10^{-2}$ $5.6 \cdot 10^{-3}$	$2.1 \cdot 10^{-2}$ $4.8 \cdot 10^{-3}$	$2.1 \cdot 10^{-2}$ $4.6 \cdot 10^{-3}$	$2.7 \cdot 10^{-2}$ $3.9 \cdot 10^{-3}$
p=50021	$5.4 \cdot 10^{-3}$ $1.7 \cdot 10^{-3}$	$6.3 \cdot 10^{-3}$ $1.8 \cdot 10^{-3}$	$5.6 \cdot 10^{-3}$ $1.5 \cdot 10^{-3}$	$6.1 \cdot 10^{-3}$ $1.5 \cdot 10^{-3}$	$8.5 \cdot 10^{-3}$ $1.3 \cdot 10^{-3}$
p=500009	$0.99 \cdot 10^{-3}$ $4.2 \cdot 10^{-4}$	$2.4 \cdot 10^{-3}$ $5.2 \cdot 10^{-4}$	$2.5 \cdot 10^{-3}$ $5.0 \cdot 10^{-4}$	$2.6 \cdot 10^{-3}$ $4.2 \cdot 10^{-4}$	$2.5 \cdot 10^{-3}$ $4.5 \cdot 10^{-4}$
p=5000011	$4.4 \cdot 10^{-4}$ $1.8 \cdot 10^{-4}$	$5.7 \cdot 10^{-4}$ $1.5 \cdot 10^{-4}$	$6.0 \cdot 10^{-4}$ $1.8 \cdot 10^{-4}$	$8.8 \cdot 10^{-4}$ $1.2 \cdot 10^{-4}$	$8.5 \cdot 10^{-4}$ $1.4 \cdot 10^{-4}$

Table 1: Max. and mean deviation, lines through the origin in $\mathbb{F}_p^2$.

	$\delta_0^{(\max)}$ $\delta_0^{(\mathrm{av.})}$	$\delta_1^{(\max)}$ $\delta_1^{(\mathrm{av.})}$	$\delta_2^{(\max)}$ $\delta_2^{(\mathrm{av.})}$	$\delta_3^{(\max)}$ $\delta_3^{(\mathrm{av.})}$	$\delta_4^{(\max)}$ $\delta_4^{(\mathrm{av.})}$
p=503	$3.7 \cdot 10^{-2}$ $2.7 \cdot 10^{-3}$	$3.9 \cdot 10^{-2}$ $3.1 \cdot 10^{-3}$	$4.1 \cdot 10^{-2}$ $4.0 \cdot 10^{-3}$	$5.0 \cdot 10^{-2}$ $4.5 \cdot 10^{-3}$	$5.2 \cdot 10^{-2}$ $5.5 \cdot 10^{-3}$
p=5003	$1.4 \cdot 10^{-2}$ $0.80 \cdot 10^{-3}$	$1.1 \cdot 10^{-2}$ $0.18 \cdot 10^{-3}$	$1.6 \cdot 10^{-2}$ $1.3 \cdot 10^{-3}$	$1.6 \cdot 10^{-2}$ $1.5 \cdot 10^{-3}$	$1.6 \cdot 10^{-2}$ $1.8 \cdot 10^{-3}$
p=50021	$3.9 \cdot 10^{-3}$ $3.1 \cdot 10^{-4}$	$4.0 \cdot 10^{-3}$ $3.0 \cdot 10^{-4}$	$4.2 \cdot 10^{-3}$ $4.2 \cdot 10^{-4}$	$4.5 \cdot 10^{-3}$ $4.9 \cdot 10^{-4}$	$5.9 \cdot 10^{-3}$ $5.8 \cdot 10^{-4}$
p=500009	$1.4 \cdot 10^{-3}$ $0.87 \cdot 10^{-4}$	$1.3 \cdot 10^{-3}$ $0.90 \cdot 10^{-4}$	$1.5 \cdot 10^{-3}$ $1.3 \cdot 10^{-4}$	$1.5 \cdot 10^{-3}$ $1.5 \cdot 10^{-4}$	$1.6 \cdot 10^{-3}$ $1.6 \cdot 10^{-4}$

Table 2: Max. and mean deviation, affine lines in $\mathbb{F}_p^2$.

Note that the above data are consistent with a $p^{-1/2}$-decay of the deviations, both for the SL_2 and the ASL_2 case. For the ASL_2 case this is in agreement with Remark 2 and the Ramanujan-Petersson conjecture that $\beta(1,2) = -\frac{1}{2}$. For the SL_2 case the tables might suggest that at least when Ω sufficiently "nice", the exponent in the error term in Theorem 2 is not optimal.

References

[COU] L. Clozel, H. Oh and E. Ullmo, Hecke operators and equidistribution of Hecke points, Inventiones Math., **144** (2001), 327–351.

[EM] N. D. Elkies and C. T. McMullen, Gaps in $\sqrt{n}$ mod 1 and ergodic theory, preprint, 2002. [Available electronically at: http://abel.math.harvard.edu/~ctm/papers/index.html]

[EsM] A. Eskin and C. T. McMullen, Mixing, counting and equidistribution in Lie groups, Duke Math. J., **71** (1993), 181–209.

[FF] L. Flaminio and G. Forni, Invariant distributions and time averages for horocycle flows, to appear in Duke Math. J., [Available electronically at: http://www-gat.univ-lille1.fr/~flaminio/]

[GO] Wee Teck Gan and Hee Oh, Equidistribution of integer points on a family of homogeneous varieties: a problem of Linnik, Compositio Math., **136** (2003), 323–352.

[KS] H. H. Kim and P. Sarnak, Refined estimates towards the Ramanujan and Selberg conjectures, appendix to H. H. Kim, Functoriality for the exterior square of GL_4 and symmetric fourth of GL_2, J. Amer. Math. Soc., **16** (2003), 139–183.

[KM] D. Y. Kleinbock and G. A. Margulis, Bounded orbits of nonquasiunipotent flows on homogeneous spaces, Sinaĭ's Moscow Seminar on Dynamical Systems, Amer. Math. Soc. Transl. Ser., **171**, Providence, RI, 1996, 141–172.

[L] Wenzhi Luo, Rational points on complete intersections over $\mathbf{F}_p$, Internat. Math. Res. Notices (1999), 901–907.

[M1] J. Marklof, The n-point correlations between values of a linear form, Ergod. Th. & Dynam. Sys. **20** (2000), 1127–1172.

[M2] J. Marklof, Pair correlation densities of inhomogeneous quadratic forms, preprint 2000/2002, to appear in *Ann. of Math.*

[MS] A. E. Mazel and Ya. G. Sinai, A Limiting Distribution Connected with Fractional Parts of Linear Forms. *Ideas and Methods in Mathematical Analysis, Stochastics and Applications,* Vol. 1. Eds. S. Albeverio *et al.* 1992, pp. 220–229.

[N] T. Nagell, Introduction to Number Theory, John Wiley & Sons, Inc., New York, 1951.

[O] Hee Oh, Uniform pointwise bounds for matrix coefficients of unitary representations and applications to Kazhdan constants, Duke Math. J., **113** (2002), 133–192.

[Sa1] P. Sarnak, Asymptotic behavior of periodic orbits of the horocycle flow and Eisenstein series, Comm. Pure Appl. Math. **34** (1981), 719–739.

[Sa2] P. Sarnak, Diophantine problems and linear groups, in *Proceedings of the International Congress of Mathematicians,* Vol. I, II (Kyoto, 1990), Math. Soc. Japan, 1991, 459–471.

[Si] C. L. Siegel, Lectures on the Geometry of Numbers, Springer-Verlag, Berlin-Heidelberg-New York, 1989.

[Sh] N. Shah, Limit distributions of expanding translates of certain orbits on homogeneous spaces, Proc. Indian Acad. Sci. (Math. Sci.) **106** (1996), 105–125. [Available electronically at: www.arXiv.org.]

[St] A. Strömbergsson, On the uniform equidistribution of long closed horocycles, preprint, 2003.

[StV] A. Strömbergsson and A. Venkatesh, volumes.mws, a Maple file available at www.math.uu.se/˜astrombe/computations.html.

[T] M. Tadić, Classification of unitary representations in irreducible representations of general linear group (non-Archimedean case), Ann. Sci. École Norm. Sup., **19** (1986), 335–382.

[Z] D. Zagier, Eisenstein series and the Riemann zeta function, in *Automorphic Forms, Representation Theory and Arithmetic,* Tata Institute (Bambay), Springer-Verlag, 1981, pp. 275-301.

(A.S.) Dept. of Mathematics, Box 480,
Uppsala Univ., S-75106 Uppsala, Sweden.
astrombe@math.uu.se

(A.V.) Dept. of Mathematics, MIT,
77 Massachusetts Ave., Cambridge,
MA 02139, USA.
akshayv@math.mit.edu