Applications of measure rigidity of diagonal actions

Manfred Einsiedler *

Abstract. Furstenberg and Margulis conjectured classifications of invariant measures for higher rank actions on homogeneous spaces. We survey the applications of the partial measure classifications result by Einsiedler, Katok, and Lindenstrauss to number theoretic problems.

Mathematics Subject Classification (2000). Primary 37A45; Secondary 37D40, 11J13.

Keywords. invariant measures, entropy, homogeneous spaces, Littlewood’s conjecture, diophantine approximation on fractals, distribution of periodic orbits, ideal classes, divisibility in integer Hamiltonian quaternions.

1. Introduction

The interaction between the theory of dynamical systems and number theory, and in particular of the theory of diophantine approximation, has a long and fruitful history. In particular, the study of the action of subgroups $H < \text{SL}_n(\mathbb{R})$ on the quotient $X_n = \text{SL}_n(\mathbb{Z}) \backslash \text{SL}_n(\mathbb{R})$ is often intimately linked to number theoretic problems.

For instance G. A. Margulis used in the late 1980’s the subgroup

$$\text{SO}(2,1)(\mathbb{R})^0 < \text{SL}_3(\mathbb{R})$$

acting on

$$X_3 = \text{SL}_3(\mathbb{Z}) \backslash \text{SL}_3(\mathbb{R})$$

by right translation to prove the long-standing Oppenheim conjecture concerning the values $Q(\mathbb{Z}^n)$ of an indefinite quadratic form in $n \geq 3$ variables, see [38]. Here the acting group $\text{SO}(2,1)(\mathbb{R})^0$ is (locally isomorphic to $\text{SL}_2(\mathbb{R})$ and so is) a simple non-compact subgroup of $\text{SL}_3(\mathbb{R})$ that is generated by unipotent one-parameter subgroups. Here a **unipotent one-parameter subgroup** is the image of a homomorphism $u : \mathbb{R} \to \text{SL}_n(\mathbb{R})$ given by $u(t) = \exp(tm)$ for $t \in \mathbb{R}$ and some given nilpotent matrix $m \in \text{Mat}_n(\mathbb{R})$.

*This research has been supported by the NSF (0554373) and the SNF (200021-127145).
Due to the work of Ratner [44, 45] the dynamics of $H$ on $X_n$ is to a large extent understood if $H$ is generated by unipotent one-parameter subgroups. These theorems and their extensions by Dani, Margulis, Mozes, Shah, and others, have found numerous applications in number theory and dynamics. We refer to [32], [40], and [46] for more details on these important topics.

These notes concern the dynamics of the diagonal subgroup $A$ of $\text{SL}_n(\mathbb{R})$, with the aim to explain the many connections between number theory and the action of $A$ on $X_n$ (or similar actions). We hope that the compilation of these applications will serve as a motivation to find new connections.

Before we list the applications let us briefly describe the dynamics of the diagonal subgroup. First we need to point out that the dynamical properties of a one-parameter subgroup $a(t)$ of $A$ is quite different from the dynamical properties of a unipotent one-parameter subgroup. For instance if $n = 2$ then the dynamical system given by right translation of the diagonal elements

$$a(t) = \begin{pmatrix} e^{t/2} & 0 \\ 0 & e^{-t/2} \end{pmatrix} = \text{diag}(e^{t/2}, e^{-t/2})$$

on $X_2$ is precisely the geodesic flow on the unit tangent bundle of the modular surface $M = \text{SL}_2(\mathbb{Z}) \backslash \mathbb{H}$. This flow is hyperbolic and one can find, e.g. by using the Anosov shadowing lemma, an abundance of arbitrarily weird orbits. We refer to [31] for the theory of hyperbolic flows and to [18, §9.7] for a discussion of $A$-invariant measures on $X_2$. This should be contrasted with the dynamics of the horocycle flow, i.e. the dynamics of the unipotent one-parameter subgroup $u(t) = \begin{pmatrix} 1 & t \\ 0 & 1 \end{pmatrix}$ on $X_2$ where every orbit is either periodic or is equidistributed in $X_2$ with respect to the Haar (or Liouville) measure, see [4] and [18, §11.7].

However, if $n \geq 3$ and $A$ denotes the full $(n - 1)$-dimensional subgroup, then it is expected that the orbits are better behaved. For instance, we have the following conjecture of G. A. Margulis.

**Conjecture 1.1.** Let $n \geq 3$ and let

$$A = \{ \text{diag}(a_1, \ldots, a_n) : a_1, \ldots, a_n > 0, a_1 \cdots a_n = 1 \}.$$  

Then any $x \in X_n = \text{SL}_n(\mathbb{Z}) \backslash \text{SL}_n(\mathbb{R})$ for which $xA$ has compact closure in $X_n$ must actually belong to a periodic (i.e. compact) orbit.

The problem of classifying all $A$-invariant measures on $X_n$ for $n \geq 3$ is strongly related to the study of orbits\(^2\). In fact, by the pointwise ergodic theorem the time-average of a function over the orbit of a (typical) point approximates the integral of the function with respect to an invariant measure. Here is the analogous conjecture for invariant measures.

\(^1\)apart from technical difficulties arising from the presence of the cusp

\(^2\)Conjecture 1.2 implies Conjecture 1.1, but in contrast to the case of unipotent dynamics an equidistribution result for $A$-orbits is not conjectured.
Conjecture 1.2. Let \( n \geq 3 \) and let \( A \) be as above. Then any \( A \)-invariant and ergodic probability measure on \( X_n \) is necessarily the normalized Haar measure on a finite volume orbit \( xH \) of an intermediate group \( A \subseteq H \subseteq SL_n(\mathbb{R}) \).

However, we also would like to mention the simplest case of such a conjectured classification result. Furstenberg proved in [21] that the full torus \( T = \mathbb{R}/\mathbb{Z} \) and certain finite sets of rational points are the only closed sets in \( T \) that are invariant under \( x \to 2x \) and \( x \to 3x \). The related question for invariant measures is a famous conjecture also due to Furstenberg (unpublished).

Conjecture 1.3. Let \( \mu \) be an invariant and ergodic probability measure on \( T = \mathbb{R}/\mathbb{Z} \) for the joint action of \( x \to 2x \) and \( x \to 3x \). Then either \( \mu \) equals the Lebesgue measure or must have finite support (consisting of rational numbers).

These conjectures and its counterparts on similar homogeneous spaces are still open, we refer to [14] for related more general versions of this conjecture. What is known towards Conjecture 1.2 is the following theorem which we obtained in joint work with A. Katok and E. Lindenstrauss [12].

Theorem 1.4. Let \( n \geq 3 \). Then an \( A \)-invariant and ergodic probability measure \( \mu \) on \( X_n \) either equals the normalized Haar measure on a closed finite volume orbit \( xH \) of an intermediate group \( A \subset H \subseteq SL_n(\mathbb{R}) \) or the measure-theoretic entropy \( h_\mu(a) \) vanishes for all \( a \in A \). If \( n \) is a prime number, then necessarily \( H = SL_n(\mathbb{R}) \).

This theorem is the analogue to the theorem of Rudolph [48] towards Conjecture 1.3. Moreover, it is related to works of A. Katok, Spatzier, and Kalinin [29, 30, 27, 28] and uses arguments both from our joint work with A. Katok [11] and the paper of E. Lindenstrauss [36] on the Arithmetic Quantum Unique Ergodicity conjecture. We do not want to describe the history of the theorem in detail and instead refer to [14].

Theorem 1.4 reduces the problem to understanding the case where entropy is zero. Depending on the application, this unsolved problem is avoided by showing that the measure in the application has positive entropy. However, this sometimes (but not always) forces extra conditions in the application. In these cases the theorem in the application would improve if one could show that an ergodic measure with vanishing entropy must be the volume measure on a periodic \( A \)-orbit \( xA \).

Theorem 1.4 has been generalized (technically speaking to all maximal \( \mathbb{R} \) resp. \( \mathbb{Q}_p \)-split diagonal subgroups acting on any quotient of an \( S \)-algebraic group). However, for this care must be taken as e.g. no such theorem can be true for the two-parameter diagonal subgroup \( A \) on the space \( SL_2(\mathbb{Z}) \times SL_2(\mathbb{Z}) \setminus SL_2(\mathbb{R}) \times SL_2(\mathbb{R}) \), as any product of two invariant measures for the geodesic flow would be an invariant measure for \( A \). Moreover, this scenario can hide e.g. inside \( \Gamma \setminus SL_2(\mathbb{R}) \). Whether or not this is an issue crucially depends on the lattice \( \Gamma \), which stands in contrast to the theorems concerning subgroups generated by unipotent subgroups where the precise nature of the lattice is not that important. We refer to [14] for the precise formulation and more details.

Here is the list of applications that we will discuss.
• Arithmetic Quantum Unique Ergodicity, see §2
• Diophantine approximation for points (and vectors) in fractals, see §3
• Non-uniformity of bad approximations of $n\alpha$, see §4
• Littlewood’s conjecture, see §5
• Compact orbits and ideal classes, see §6
• Counting rational points in a certain variety, see §7
• Divisibility properties of Hamiltonian quaternions, see §8

We also want to refer to the lecture notes [15] for the Clay summer school in Pisa in 2007 which explain in detail the (otherwise not so readily available) background of the papers [11, 12] as well as their content, and discusses two applications. Finally, we also wrote together with E. Lindenstrauss a joint survey [14] on this topic, which explains in detail the general conjectures and partial measure classifications and again some of the applications. In contrast to these surveys and lecture notes, we want to give here a description of all the applications and try to point out most concretely how these topics are connected to diagonal actions. For these applications we do not have to consider the most general theorems as all applications concern quotients of the group $\text{SL}_n$ (or products of the form $\text{SL}_n \times \cdots \times \text{SL}_n$). This is unfortunate, as the theorems (in appropriate formulations) are more general.

I would like to thank my co-authors A. Katok, E. Lindenstrauss, Ph. Michel, and A. Venkatesh for the many collaborations on these subjects.

2. Arithmetic Quantum Unique Ergodicity

Historically the first application of a partial measure classification for diagonal flows (outside of ergodic theory) concerns the distributional properties of Hecke-Maass cusp forms $\phi$ on $M = \text{SL}_2(\mathbb{Z}) \backslash \mathbb{H}$ and similar quotients of the hyperbolic plane $\mathbb{H}$ by congruence subgroups. Here a Maass cusp form is a smooth function $\phi$ on $M$ which is an eigenfunction of the hyperbolic Laplace operator $\Delta_M$ and also belongs to $L^2(M)$ — we will always assume the normalization $||\phi||_2 = 1$. A Hecke-Maass cusp form is a Maass cusp form that in addition is also an eigenfunction of the Hecke operators $T_p$ for all $p$.

Rudnick and Sarnak [47] conjectured that for any sequence of Maass cusp forms $\phi_i$ on $M$ for which the eigenvalues go to infinity the probability measures defined by $|\phi_i|^2\text{dvol}_M$ converges in the weak* topology to the uniform measure $\text{dvol}_M$. These conjectures are of interest to mathematical physics as well as number theory. In quantum physics eigenfunctions of $\Delta$ are energy states of a free (spinless, non-relativistic) quantum particle, moving in the absence of external forces on $M$. In number theory the eigenfunctions are of central importance due to many connections between them and the theory of $L$-functions. We refer to the survey [50] and the more recent [49] for more details.
After a conditional proof of the following theorem by Watson [59] relying on the 
generalized Riemann hypothesis, Lindenstrauss [36] used a partial measure classification to show the equidistribution except for the possibility that the limit measure may not be a probability measure (or even the zero measure). Soundararajan [56] complemented the proof of Lindenstrauss showing that the limit measure must indeed be a probability measure. Together this gives the following unconditional theorem.

**Theorem 2.1** (Arithmetic Quantum Unique Ergodicity). Let $M = \Gamma \backslash \mathbb{H}$, with $\Gamma$ a congruence lattice over $\mathbb{Q}$. Then $|\phi_i|^2 \, \text{dvol}_M$ converges in the weak$^*$ topology to $\text{dvol}_M$ as $i \to \infty$ for any sequence of Hecke-Maass cusp forms for which the Maass eigenvalues $\lambda_i \to -\infty$ as $i \to \infty$.

The connection of this problem to the problem of classifying invariant measures on $X = \Gamma \backslash \text{SL}_2(\mathbb{R})$ with respect to the geodesic flow is well motivated due to the interpretation of the Maass forms on $M$ as the distribution of quantum particles on the surface $M$ with a given energy (which up to a constant equals the eigenvalue for the Laplace operator) and the study of the semi-classical limit (corresponding to the limit where the energy goes to infinity). Moreover, Shnirelman [55], Zelditch [61] and Coin-de-Verdeire [6] used this connection before to show the so-called Quantum Ergodicity. This theorem says that for any compact quotient $\Gamma \backslash \mathbb{H}$ and a subsequence of all eigenfunctions of density one, the measures $|\phi_i|^2 \, \text{dvol}_M$ indeed converge to $\text{dvol}_M$. Part of this proof is the construction of a so-called micro-local lift of a weak$^*$ limit, which is a measure $\mu$ on the unit tangent bundle $X = \Gamma \backslash \text{SL}_2(\mathbb{R})$ that is invariant under the geodesic flow.

The additional assumption in Theorem 2.1 that $\phi_i$ is also an eigenfunction of the Hecke-operators can be used to prove additional properties of the micro-local lift. Indeed, Bourgain and Lindenstrauss [2] show that a micro-local lift must have the property that all of its ergodic components have positive entropy. Here the positivity of entropy is shown by proving that the measure of a small ball $B_\epsilon(x)$ for $x \in X$ decays like $\ll \epsilon^{1+\delta}$ for $\delta = \frac{2}{9}$. The ‘trivial bound’ in this case is $\ll \epsilon$ since the measure is known to be invariant under the one-dimensional subgroup $A$ consisting of diagonal elements. Any improvement of the form $\ll \epsilon^{1+\delta}$ for some $\delta > 0$ shows positivity of entropy of almost all ergodic components.

Furthermore, Lindenstrauss [36] also shows that such a micro-local lift of a sequence of Hecke-Maass cusp forms has an additional recurrence property under the $p$-adic group $\text{SL}_2(\mathbb{Q}_p)$ for any $p$ — this is a much weaker requirement than invariance but suffices due to the following theorem [36].

**Theorem 2.2**. Let $\Gamma$ be a congruence lattice over $\mathbb{Q}$, let $X = \Gamma \backslash \text{SL}_2(\mathbb{R})$ and let $\mu$ be a probability measure satisfying the following properties:

(I) $\mu$ is invariant under the geodesic flow,

(E) the entropy of every ergodic component of $\mu$ is positive for the geodesic flow, and

(R) $\mu$ is Hecke $p$-recurrent for a prime $p$. 
Then $\mu$ is the uniform Haar measure $m_X$ on $X$.

The proof of this theorem uses an idea from [11] and also an idea from the work of Ratner on the rigidity of the horocycle flow [42, 43]. The latter is surprising as the measure $\mu$ under consideration has a-priori very little structure with respect to the horocycle flow.

We refer to the lecture notes [17], which explain carefully the arguments in [2] and [36] (with the exception of the proof of Theorem 2.2).

After the work of Lindenstrauss, Silberman and Venkatesh [53] have generalized this approach to quotients of $\text{SL}_n(\mathbb{R})$ by congruence lattices arising from division algebras, where the degree $n$ of the division algebra is assumed to be a prime number. (In this case Theorem 1.4 holds in the same way.)

3. Diophantine approximation for points in fractals

The connection between the continued fraction expansion and the geodesic flow on $X_2 = \text{SL}_2(\mathbb{Z}) \backslash \text{SL}_2(\mathbb{R})$ goes back to work of Artin [1], see also [51, 52]. This link between Diophantine approximation of real numbers and dynamics on homogeneous spaces has been extended to higher dimension by Dani [3] and since then has been used successfully by many authors. We will recall this connection below.

In the theory of metric Diophantine approximations, one wishes to understand how well vectors in $\mathbb{R}^d$ can be approximated by rational vectors. In particular, we say $v \in \mathbb{R}^d$ is well approximable if for any $c > 0$ there are infinitely many nonzero integers $q$ for which there exists an integer vector $p \in \mathbb{Z}^d$ with

$$\|v - \frac{1}{q} p\| \leq \frac{c}{q^{1+\frac{1}{d}}}.$$  

Similarly we say $v$ is badly approximable if there exists a constant $c > 0$ such that

$$\|v - \frac{1}{q} p\| \geq \frac{c}{q^{1+\frac{1}{d}}}.$$  

for all $q \in \mathbb{Z}$ and $p \in \mathbb{Z}^d$. We will write WA (resp. BA) for the set of well approximable (resp. badly approximable) vectors. It is well known that almost every $v$ is well approximable, but that the set of badly approximable vectors is also in many ways big — e.g. W. Schmidt has shown that the set of badly approximable vectors has full Hausdorff dimension.

Recently, the question how special submanifolds or fractals within $\mathbb{R}^d$ intersect the set of badly or well approximable vectors (as well as other classes of vectors with special Diophantine properties) has attracted attention. For instance, it was shown for the Cantor set $C \subset [0,1]$ in [33] and [34], that the dimension of $C \cap \text{BA}$ is full, i.e. equals $\log 2/\log 3$. However, until recently little was known about the intersection of WA with fractals. In joint work [10] with L. Fishman and U. Shapira we obtained the following application of Theorem 2.2.
**Theorem 3.1.** Almost any point in the middle third Cantor set (with respect to the natural measure) is well approximable and moreover its continued fraction expansion contains all patterns.

We would like to point out that the special invariance properties that the Cantor set has, are actually crucial for the proof of Theorem 3.1 while the result concerning the intersection of the Cantor set with BA are much more general. The same method that gives Theorem 3.1 can also be used for $d = 2$ together with Theorem 1.4 and leads to the following theorem.

**Theorem 3.2.** Let $A : \mathbb{R}^2/\mathbb{Z}^2 \to \mathbb{R}^2/\mathbb{Z}^2$ be a hyperbolic automorphism, induced by the linear action of a matrix $A \in \text{SL}_2(\mathbb{Z})$ and let $\mu$ be a probability measure which is invariant and ergodic with respect to $A$, and has positive dimension. Then $\mu$ almost any $v \in \mathbb{R}^2/\mathbb{Z}^2$ is well approximable.

To see the connection between these two theorems and Theorem 2.2 resp. Theorem 1.4 we need to recall the interpretation of $X_n = \text{SL}_n(\mathbb{Z}) \setminus \text{SL}_n(\mathbb{R})$ as the space of unimodular lattices in $\mathbb{R}^n$. In fact, we may identify the identity coset $\text{SL}_n(\mathbb{Z})$ with the unimodular (i.e. covolume one) lattice $\Lambda = \mathbb{Z}^n$. More generally, we identify the coset $\text{SL}_n(\mathbb{Z})g$ with the lattice $\Lambda = \mathbb{Z}^ng$. This gives an isomorphism between $X_n$ and the space of unimodular lattices in $\mathbb{R}^n$, and makes it possible to classify compact subsets by the following geometric property.

**Theorem 3.3** (Mahler’s compactness criterion). A subset $C \subset X_n$ is bounded (i.e. its closure is compact) if and only if there exists $\epsilon > 0$ such that for any lattice $\Lambda \in C$, $\Lambda \cap B_{\epsilon}(0) = \emptyset$ i.e. if and only if there exists a uniform lower bound for the lengths of nonzero vectors belongings to points in $C$.

This gives the basis of the dynamical interpretation of badly approximable vectors $v$ (used as row vector) in terms of the orbit of the associated lattice

$$\Lambda_v = \mathbb{Z}^{d+1} \begin{pmatrix} I_d & 0 \\ v & 1 \end{pmatrix}$$

with respect to the generalization of the geodesic flow defined below. Here we write $I_d$ for the $d \times d$-identity matrix.

**Corollary 3.4.** We define the diagonal elements

$$a_t = \begin{pmatrix} e^{t/d} I_d & 0 \\ 0 & e^{-t} \end{pmatrix}$$

for any $t \in \mathbb{R}$. Then a vector $v \in \mathbb{R}^d$ is badly approximable if and only if the forward orbit

$$\{ \Lambda_v a_t : t \geq 0 \}$$

of the lattice $\Lambda_v$ associated to $v$ is bounded in $X_{d+1}$. 

Let us indicate one direction of this characterization. If \( v \) is badly approximable as in (1) and \( t \geq 0 \), then the elements of the lattice \( \Lambda_v a_t \) are of the form

\[
( (p - qv)e^{t/d}, e^{-t}q )
\]

We claim that any non-zero such element cannot be closer to the origin in \( \mathbb{R}^{d+1} \) than \( c \). Otherwise, we derive from \( t \geq 0 \) that \( q \neq 0 \) and by taking the product of the norm of \( (p - qv)e^{t/d} \) and of the \( d \)-th root of \( e^{-t}q \) that \( q^{1/d} ||p - qv|| < c \) — a contradiction to (1). The opposite implication is similar.

Let us indicate now the relationship between Theorem 2.2 and Theorem 3.1. Write \( \nu_C \) for the uniform measure on the middle third Cantor set. We may embed \( \nu_C \) as a measure on \( X_2 \) by push-forward via the map \( v \rightarrow \Lambda_v \). By Corollary 3.4 what we would like to show is that for \( \nu_C \)-a.e. point the orbit under the geodesic flow is unbounded.

To better phrase the special invariance properties that the Cantor set has, it makes sense to introduce the 3-adic extension of \( X_2 \). One can check that

\[
X_2 \cong \text{SL}_2(\mathbb{Z}[\frac{1}{3}]) \backslash \text{SL}_2(\mathbb{R}) \times \text{SL}_2(\mathbb{Q}_3)/\text{SL}_2(\mathbb{Z}_3),
\]

so that we should think of \( \widetilde{X}_2 = \text{SL}_2(\mathbb{Z}[\frac{1}{3}]) \backslash \text{SL}_2(\mathbb{R}) \times \text{SL}_2(\mathbb{Q}_3) \) as an extension of \( X_2 \) by compact fibers isomorphic to \( \text{SL}_2(\mathbb{Z}_3) \).

We note that

\[
\text{SL}_2(\mathbb{Z}[\frac{1}{3}]) \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix} \begin{pmatrix} 3 & 0 \\ 0 & 3^{-1} \end{pmatrix} = \text{SL}_2(\mathbb{Z}[\frac{1}{3}]) \begin{pmatrix} 1 & 0 \\ 9v & 1 \end{pmatrix},
\]

which shows that right-multiplication by the diagonal element \( \begin{pmatrix} 3 & 0 \\ 0 & 3^{-1} \end{pmatrix} \) corresponds to multiplying \( v \) by 9. As the Cantor set has a special relationship with respect to multiplication by 3 (or equivalently ternary digit expansions), this can be exploited and one can construct an invariant measure \( \widetilde{\nu}_C \) on \( \widetilde{X}_2 \) for the map that multiplies on the right — both in the real and 3-adic component — by \( \begin{pmatrix} 3 & 0 \\ 0 & 3^{-1} \end{pmatrix} \).

However, this dynamical system is different from the extension of the geodesic flow \( a_t \), which is just right multiplication by the diagonal element \( \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix} \) in the real component. Taking the average of \( \widetilde{\nu}_C \) along the orbit under \( a_t \) one obtains a measure that is invariant under the diagonal subgroup — both in the real component and the 3-adic component. To this limit measure \( \mu \) one can apply Theorem 2.2. The recurrence condition is assured since \( \mu \) is actually invariant under a non-compact subgroup of \( \text{SL}_2(\mathbb{Q}_3) \). The entropy assumption is satisfied in the weaker sense that the entropy of \( \mu \) is positive — this is a consequence of the fact that \( \nu_C \) had positive dimension.

From this, we conclude not necessarily that \( \mu \) equals the Haar measure but at least that it contains the Haar measure as one of the ergodic components. Clearly the Haar measure has non-compact support, and this can be used to deduce\(^3\) Theorem 3.1.

\(^3\)The cautious reader may notice that what we said implies only that the quantity \( c \) as in (1)
4. Non-uniformity of bad approximations

Recall that every irrational $x \in [0,1]$ can be written as a continued fraction. The digits of the continued fraction expansion relates to the discussion of the Diophantine approximation above. In fact, $x$ is badly approximable if and only if the digits $a_n(x)$ of the expansion are bounded. If $x$ is badly approximable, then the quantity $c(x) = \limsup a_n(x)$ measures the extent to which $x$ is badly approximable. In this sense, the next theorem says that the sequence $x, 2x, \ldots, nx, \ldots$ cannot be uniformly badly approximable.

**Theorem 4.1.** If we denote for $v \in [0,1]$, $c(v) = \limsup a_n(v)$ where $a_n(v)$ are the coefficients in the continued fraction expansion of $v$, then for any irrational $v \in [0,1]$, $\sup_n c(n^2v) = \infty$, where $n^2v$ is calculated modulo 1.

This is also joint work with L. Fishman and U. Shapira [10]. We would like to point out that this relates to a conjecture of M. Boshernitzan, who reported to us that a stronger version of Theorem 4.1 holds for the special case of quadratic irrationals.

The proof of Theorem 4.1 is similar in spirit to the proof of Theorem 3.1, but this time takes place on $X_{2,A} = SL_2(\mathbb{Q}) \backslash SL_2(\mathbb{A})$ where multiplication of $v$ by $n^2$ can be converted to right multiplication by the matrix \( \begin{pmatrix} n & 0 \\ 0 & n^{-1} \end{pmatrix} \) (in every component). These elements together with the real diagonal subgroup give a big subgroup $A'$ of the full group $A_\mathbb{A}$ of adelic points of the diagonal subgroup, more precisely the quotient of $A_\mathbb{A}$ by $A'$ is compact. In this theorem there is no mention of entropy or dimension due to the following theorem by E. Lindenstrauss [35] (which is the combination of Theorem 2.2 and the method in [2]).

**Theorem 4.2.** The action of the group, $A_\mathbb{A}$, of adelic points of the diagonal subgroup in $SL_2$ on $X_{2,A} = SL_2(\mathbb{Q}) \backslash SL_2(\mathbb{A})$ is uniquely ergodic.

5. Littlewood’s conjecture

Historically the second application of a partial measure classification result for diagonal subgroups (in this case Theorem 1.4) has been a partial result towards Littlewood’s conjecture.

**Conjecture 5.1** (Littlewood (c. 1930)). For every $\alpha, \beta \in \mathbb{R}$,

$$\liminf_{n \to \infty} n\|n\alpha\|n\|\beta\| = 0,$$

where $\|w\| = \min_{n \in \mathbb{Z}} |w - n|$ is the distance of $w \in \mathbb{R}$ to the nearest integer.

cannot be uniform for a.e. point in $C$, but with a bit more work, using only ergodicity of the Haar measure, one really obtains a proof.
Similar to Corollary 3.4 one can also show the following characterization of Littlewood’s conjecture in dynamical terms.

**Proposition 5.2.** \((\alpha, \beta)\) satisfy (2) if and only if the orbit 
\[ \Lambda_{\alpha, \beta} a_{s,t} = \text{SL}(3, \mathbb{Z}) \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ \alpha & \beta & 1 \end{pmatrix} a_{s,t} \]
under the semigroup
\[ A^+ = \{ a(s, t) : s, t \geq 0 \} \quad a(s, t) = \begin{pmatrix} e^t & 0 & 0 \\ 0 & e^s & 0 \\ 0 & 0 & e^{-t-s} \end{pmatrix} \]
is unbounded in \(X_3 = \text{SL}(3, \mathbb{Z}) \setminus \text{SL}(3, \mathbb{R})\).

Together with Theorem 1.4 this leads to the following theorem.

**Theorem 5.3** ([12, Theorem 1.5]). For any \(\delta > 0\), the set\(^4\)
\[ \Xi_{\delta} = \left\{ (\alpha, \beta) \in [0, 1]^2 : \liminf_{n \to \infty} n\|n\alpha\|\|n\beta\| \geq \delta \right\} \]
has zero upper box dimension\(^5\). In particular, \(\bigcup_{\delta > 0} \Xi_{\delta}\) has zero Hausdorff dimension.

We refer to [12] or to [15] for an explanation on how the entropy assumption in Theorem 1.4 is converted to the box dimension result above. A full solution of either Conjecture 1.1 or Conjecture 1.2 would imply Conjecture 5.1. The same method can also be used to obtain a partial result towards a conjecture of B. de Mathan and O. Teulié [5]. They conjectured\(^6\) that for every prime number \(p\), for every \(u \in \mathbb{R}\) and \(\epsilon > 0\)
\[ \left| qu - q_0 \right| < \frac{\epsilon}{q|q|_p} = \frac{\epsilon}{q'} \quad \text{for infinitely many pairs } (q, q_0) \in \mathbb{Z}^2, \]
where \(q = q'p^k\) for some \(k \geq 0\), \(q'\) is coprime to \(p\), and \(|q|_p = 1/p^k\) denotes the \(p\)-adic norm. Equivalently one can ask whether
\[ \liminf_{q \to \infty} |q| \cdot |q|_p \cdot \|qu\| = 0, \tag{3} \]
In joint work with Kleinbock [13] we have shown the following analogue to Theorem 5.3.

**Theorem 5.4.** The set of \(u \in \mathbb{R}\) which do not satisfy (3) has Hausdorff dimension zero.

\(^4\)Since (2) depends only on \(\alpha, \beta \mod 1\) it is sufficient to consider only \((\alpha, \beta) \in [0, 1]^2\).

\(^5\)i.e., for every \(\epsilon > 0\), for every \(0 < r < 1\), one can cover \(\Xi_{\delta}\) by \(O_{\delta, \epsilon}(r^{-\epsilon})\) boxes of size \(r \times r\).

\(^6\)Their conjecture is more general.
6. Compact orbits and ideal classes

Another interesting connection between the dynamics of the full diagonal subgroup $A$ on $X_n = \text{SL}_n(\mathbb{Z}) \backslash \text{SL}_n(\mathbb{R})$ and number theory arises in the study of periodic (i.e. compact) orbits of $A$ on $X_n$.

In fact, if $I \subset O_K$ is an ideal in the ring of integers of a totally real number field $K$ of degree $n$ then this ideal can give rise to a compact $A$-orbit as follows. To see this, let $\phi_1, \ldots, \phi_n : K \to \mathbb{R}$ be the complete list of Galois embeddings. Then

$$\{(\phi_1(k), \ldots, \phi_n(k)) : k \in I\} \subset \mathbb{R}^n$$

is a lattice in $\mathbb{R}^n$, which after normalization of the covolume, gives an element $\Lambda_I \in X_n$. By Dirichlet’s unit theorem, there are $n-1$ multiplicatively independent units in the ring $O_K$. Let $\xi$ be one such unit. Replacing $\xi$ by $\xi^2$ if necessary, we may assume that $\phi_i(\xi) > 0$ for all $i$. Then $a = \text{diag}(\phi_1(\xi), \ldots, \phi_n(\xi)) \in A$ satisfies

$$\{(\phi_1(k), \ldots, \phi_n(k)) : k \in I\}a = \{(\phi_1(k), \ldots, \phi_n(k)) : k \in \xi I\},$$

which shows that $\Lambda_I = \Lambda_I a$ is fixed under $a$ since $\xi I = I$ for any unit. As $A$ has $n-1$ dimensions and we have $n-1$ independent units, one obtains that $\Lambda_I A$ is an $n-1$-dimensional torus and so compact. We write $\mu_{\Lambda_I}$ for the Lebesgue measure on this torus normalized to be a probability measure and viewed as a measure on $X_n$.

One can furthermore check that two ideals give rise to the same compact orbit if and only if the two ideals are equivalent. Therefore, the number of compact $A$-orbits arising from the maximal order $O_K$ of the field is precisely the class number of the field.

The same construction shows that any ideal in any order $O$ of $K$ gives rise to a compact $A$-orbit. Allowing this more general construction one actually obtains all compact $A$-orbits. It is natural to ask how the various compact orbits for a given order distribute within $X_n$. If $n = 2$ special cases of the expected equidistribution theorem have been proven around 1960 by Linnik [37] and Skubenko [54]. The full statement has been proven by Duke [7] in 1988 using subconvexity estimates of $L$-functions. For $n = 3$ the analogue has been obtained more recently in joint work with Lindenstrauss, Michel, and Venkatesh [9].

**Theorem 6.1.** Let $K_\ell$ be a sequence of totally real degree three extensions of $\mathbb{Q}$, and let $h_\ell$ the class number of $K_\ell$. Let $x_{1,\ell}A, \ldots, x_{h_\ell,\ell}A \subset X_3$ be the periodic $A$-orbits corresponding to the ideal classes of $K_\ell$ as above. Let $\mu_\ell = \frac{1}{h_\ell} \sum \mu_{x_{1,\ell}A}$. Then $\mu_\ell$ converge in the weak* topology to the $\text{SL}(3,\mathbb{R})$ invariant probability measure $m_{X_3}$ on $X_3$.

The proof uses a combination of methods. First, subconvexity estimates of Duke, Friedlander and Iwaniec [8] imply that for certain test functions $f$, the integrals $\int_{X_3} f d\mu_\ell$ converge to the expected value (i.e. $\int_{X_3} f dm_{X_3}$). The space of these test functions is not sufficient to conclude Theorem 6.1, but can be used to deduce that $\mu_\ell$ is a probability measure (i.e. there is no escape of mass to the
Manfred Einsiedler

cusp) and that the entropy of every ergodic component in such a limiting measure is greater than an explicit lower bound. Once these two facts have been established, Theorem 1.4 gives the result.

We also refer to [9, 16] and the survey [39] for more details on this and related application.

7. Counting rational points

For the following application we fix a monic irreducible polynomial \( P(\lambda) \in \mathbb{Q}[\lambda] \) of degree \( n \). Let us assume that \( P(\lambda) \) factorizes over \( \mathbb{R} \). Let \( V \subset \text{Mat}_{nn} \) be the variety consisting of all matrices whose characteristic polynomial equals \( P(\lambda) \). Next recall that for any rational vector \( v = (\frac{p_1}{q}, \ldots, \frac{p_\ell}{q}) \) represented in lowest terms, we can define the \emph{height} as the maximum of the absolute values \( |p_i| \) and the common denominator \( q \). Zamojski [60] has proven the following asymptotic counting formula.

**Theorem 7.1.** If \( N_R \) denotes the number of rational matrices with characteristic polynomial \( P(\lambda) \) and height bounded by \( R \), then the limit

\[
\lim_{R \to \infty} \frac{N_R}{R^{n(n-1)/2+1}}
\]

exists and is positive.

This proves a new case of Manin’s conjecture (see [57, 58]) which concerns similar counting problems on more general varieties. There is already a rich history for the interaction between asymptotic counting problems and ergodic theory. Initially, only mixing in the form of the theorem by Howe and Moore was used, see for instance the influential work of Eskin and McMullen [19]. However, after Ratner proved her theorems [44] further cases of the counting problem could be handled. For instance, Eskin, Mozes, and Shah [20] have proven in 1996 the integer version of Theorem 7.1.

In all of these proofs of asymptotic counting the following equidistribution problem is of crucial importance. The variety \( V \) as above is actually a single orbit of \( \text{PGL}_n(\mathbb{R}) \), we write \( H \) for its stabilizer. Similar to the discussion in §6 the orbit \( \text{PGL}_n(\mathbb{Z})H \) of the identity coset is compact, we write \( \mu \) for the measure on \( X = \text{PGL}_n(\mathbb{Z}) \backslash \text{PGL}_n(\mathbb{R}) \) that is supported on \( \text{PGL}_n(\mathbb{Z})H \) and invariant under \( H \).

Then the counting problem of integer points in \( V \) is related to the equidistribution of the measure \( \mu g \) (obtained by applying right multiplication by \( g \)) on the space \( X \). In [20] it is shown that, at least on average, \( \mu g \) indeed equidistributes. For this the theory of unipotent dynamics was used, which at first may be surprising as \( H \) does not contain any unipotents. The key link of this problem to unipotents lies in the fact that \( \mu g \) is invariant under \( g^{-1}Hg \), which if \( g_n \to \infty \) in \( H \backslash G \) implies that any limit measure of \( \mu g_n \) is invariant under a one-parameter unipotent subgroup.

For counting rational points on homogenous varieties it is natural to replace the quotient \( X \) by the corresponding adelic quotient, as was shown in the work
of Gorodnik, Maucourant, and Oh [22]. Also in the proof of Theorem 7.1 the equidistribution of translates of a given finite volume measure on the adelic quotient \( \Gamma \backslash \text{PGL}_n(\mathbb{A}) \) is studied. However, unlike the case of counting integer points, it is no longer true that the translated measures will on average develop invariance properties under a unipotent subgroup. Roughly speaking this is because it is not true that if a sequence \( g_n \in \text{PGL}_n(\mathbb{A}) \) goes to infinity, then for some place \( p \) the projection of \( g_n \) to this place goes to infinity. Indeed, as Zamojski shows for most sequences \( g_n \) the projections stay bounded within each place. Hence the limit measures are only known to have the same invariance as the original measure \( \mu \) — invariance under a conjugate of the diagonal subgroup \( A \). Zamojski shows, similar to a part of the proof of Theorem 6.1 in [9] that a limit measure must have positive entropy (for all of its ergodic components) and so Theorem 1.4 can be applied. However, if \( n \) is not a prime number, Zamojski gives an additional argument which rules out the measures corresponding to intermediate subgroups.

8. Divisibility properties of Hamiltonian quaternions

Our last application uses an analogue of Theorem 2.2 for a quotient of the form \( \Gamma \backslash \text{PGL}_2(\mathbb{Q}_p) \times \text{PGL}_2(\mathbb{Q}_q) \) for two primes \( p \neq q \), and concerns divisibility properties of integer Hamiltonian quaternions. This is a special case of ongoing joint work with S. Mozes.

Let \( H = \mathbb{R}[i, j, k] \) be the Hamiltonian quaternions, and let \( \mathcal{O} = \mathbb{Z}[i, j, k] \) be the order consisting of integer combinations of 1 and the three imaginary units \( i, j, k \). We write \( N(a + bi + cj + dk) = a^2 + b^2 + c^2 + d^2 \) for the norm on \( H \).

Let \( p \neq 2 \) be a prime number. Then

\[
\Gamma_p = \{ \alpha \in \mathcal{O} : N(\alpha) \text{ is a power of } p \}
\]

is a multiplicative semi-group, for which \( \pm 1 \) and \( p \) generates the center \( C \). Taking the quotient by the center, one obtains a group \( \text{P} \Gamma_p = \Gamma_p/C \). As a consequence of Pall’s unique factorization theorem for elements of \( \mathcal{O} \) it follows that \( \text{P} \Gamma_p \) is virtually a free group (more concretely it contains a free group with \( \log p \) generators and index 4).

Similarly if \( p, q \neq 2 \) are two different odd prime numbers, then we define the semigroup

\[
\Gamma_{p, q} = \{ \alpha \in \mathcal{O} : N(\alpha) \text{ is a product of powers of } p \text{ and } q \}
\]

which once more gives a group \( \text{P} \Gamma_{p, q} = \Gamma_{p, q}/C \) after dividing by the center.

The group \( \text{P} \Gamma_{p, q} \) is far from being a free group. This is known, but is also shown clearly by the following theorem. For stating the theorem we need some definitions. We say an element \( \alpha \in \mathcal{O} \) appears\(^\text{7}\) in \( \beta \in \mathcal{O} \) if there exits some

\(^{7}\)We write "appears" for this notion of divisibility to distinguish this notion from a left- or right-divisibility that is sometimes considered for non-commutative rings.
ℓ, r ∈ O such that β = ℓαr. The fact that P Γ_p contains a free subgroup shows that for any fixed α ∈ Γ_p with N(α) > 1 the set
\[ \{β ∈ Γ_p : α does not appear in β and N(β) = p^k\} \]
grows exponentially with k. We say that α ∈ Γ_{p,q} is reduced if \( \frac{1}{p^i} α \notin O \) and \( \frac{1}{q^j} α \notin O \). In contrast to Γ_p we have the following theorem concerning Γ_{p,q}.

**Theorem 8.1.** Let p, q ≠ 2 be two different primes. Then for any reduced α ∈ Γ_{p,q} the set
\[ \{β ∈ Γ_{p,q} : α does not appear in β and N(β) = p^k q^k\} \]
grows sub-exponentially. That is, if \( M(k) \) is the cardinality of the set, then
\[ \lim_{k→∞} \frac{1}{k} \log M(k) = 0. \]

Let us indicate the connection between the above theorem and the dynamics of diagonal flows, which goes back to [41]. First we may choose a subgroup \( Γ \subset P Γ_{p,q} \) of finite index which does not contain the images of the elements ±i, ±j, ±k and is generated by two free subgroups of P Γ_p and P Γ_q. Then Γ is naturally a lattice in the group \( G = PGL_2(\mathbb{Q}_p) × PGL_2(\mathbb{Q}_q) \) for which a fundamental domain is given by the compact set \( F = PGL_2(\mathbb{Z}_p) × PGL_2(\mathbb{Z}_q) \).

Let \( a_p = \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} × I \), where I denotes the identity. Define \( a_q \) similarly. Since F is a fundamental domain, there exists for every \( f ∈ F \) some element \( γ ∈ Γ ∩ P Γ_p \) and some \( f' ∈ F \) for which \( fa_p = γf' \). Clearly, if \( f \) is replaced by a slight perturbation of \( f \), then \( γ \) will not change. In this sense, \( γ \) corresponds to an open subset \( O_γ \) of \( F ≃ Γ \backslash G \). More generally, if \( γ ∈ Γ \) then \( γ \) is the image of some reduced element in \( O \) which we assume has norm \( p^k q^k \) and we can define the open (and non-empty) subset
\[ O_γ = \{f ∈ F : fa_p^k a_q^k ∈ γF\}. \]

If now \( β = ℓαr \) for elements \( α, β, l, r ∈ O \) with \( N(l) = p^m q^n \), then \( f ∈ O_β \) implies that \( fa_p^m a_q^n ∈ O_α \). This has a partial converse, meaning that if \( f ∈ O_β \) satisfies \( fa_p^m a_q^n ∈ O_α \) for sufficiently small values of \( m \) and \( n \) then we deduce that \( α \) appears in \( β \).

In this sense an element \( β \) of norm \( N(β) = p^k q^k \) in which \( α \) does not appear, gives rise to a piece of an orbit under the joint action of \( a_p \) and \( a_q \) on \( Γ \backslash G \) that does not visit the open set \( Γ O_α \). If there are exponentially many such elements \( β \) as \( k → ∞ \), then one can construct (with the help of the variational principle from ergodic theory) from these many large pieces of orbits an invariant measure on \( Γ \backslash G \) with positive entropy and zero mass on the set \( O_α \). The analogue of Theorem 1.4 for the action of \( a_p \) and \( a_q \) on \( Γ \backslash G \) holds and is indeed a version of Theorem 2.2, hence we derive a contradiction and Theorem 8.1 follows.
9. Open problems

We already mentioned the main open problems: Furstenberg’s Conjecture 1.3 regarding jointly invariant probability measures for the times 2 and times 3 maps on \( T \), and Margulis’ Conjectures 1.1–1.2 regarding bounded orbits and invariant measures on \( \text{SL}_n(\mathbb{Z}) \backslash \text{SL}_n(\mathbb{R}) \) for \( n \geq 3 \). We also refer to [14] and [23] for related conjectures on the measure classification.

However, even if we allow ourselves the positive entropy assumption there are still unsolved cases where no analogue to Theorem 1.4 is known. For instance we may take a subgroup \( A' \subset A \) of dimension two within the three-dimensional diagonal subgroup \( A \subset \text{SL}_4(\mathbb{R}) \) and ask what are the \( A' \)-invariant and ergodic probability measures on \( X_4 = \text{SL}_4(\mathbb{Z}) \backslash \text{SL}_4(\mathbb{R}) \) for which some element \( a \in A' \) acts with positive entropy. The current techniques that go into Theorem 1.4 fall short in this case.

The list of the applications, discussed above, also suggests a number of open problems. For instance, Theorem 3.2 currently only holds for \( d = 2 \) and Theorem 4.1 only for \( d = 1 \). However, we certainly would expect that these hold in any dimension.

Also Theorem 6.1 currently only holds for cubic fields and the non-compact space \( X_3 \), so it is natural to ask for the same for higher dimensions or for compact quotients of \( \text{SL}_3(\mathbb{R}) \) by the units in a degree 3 division algebra over \( \mathbb{Q} \).

Another interesting question arises by comparing the argument in [10] (see §3) with Host’s theorem [24, 25].

**Conjecture 9.1.** Let \( \mu \) be a probability measure on an irreducible quotient \( X = \Gamma \backslash \text{SL}_2(\mathbb{R}) \times \text{SL}_2(\mathbb{R}) \). Suppose \( \mu \) is invariant and ergodic with respect to the action of the one-parameter diagonal subgroup \( A_1 \subset \text{SL}_2(\mathbb{R}) \times \{1\} \) of the first copy of \( \text{SL}_2(\mathbb{R}) \), and suppose \( \mu \) has positive entropy with respect to \( A_1 \). Write \( A_2 \subset \{1\} \times \text{SL}_2(\mathbb{R}) \) for the one-parameter diagonal subgroup in the second \( \text{SL}_2(\mathbb{R}) \). Then \( \mu \)-a.e. \( x \in X \) has equidistributed orbit for the action of \( A_2 \).

The theorem in [24] concerns the same problem with \( X = T \), \( A_1 \) replaced by \( \times 2 \), and \( A_2 \) replaced by \( \times 3 \). A slightly easier problem would be to generalize the related theorem of Johnson and Rudolph [26], which might look as follows.

**Conjecture 9.2.** Let \( \mu \) be a probability measure on an irreducible quotient \( X = \Gamma \backslash \text{SL}_2(\mathbb{R}) \times \text{SL}_2(\mathbb{R}) \). Suppose \( \mu \) is invariant and ergodic with respect to the action of the one-parameter diagonal subgroup \( A_1 \subset \text{SL}_2(\mathbb{R}) \times \{1\} \) of the first copy of \( \text{SL}_2(\mathbb{R}) \), and suppose \( \mu \) has positive entropy with respect to \( A_1 \). Write \( A_2 \subset \{1\} \times \text{SL}_2(\mathbb{R}) \) for the one-parameter diagonal subgroup in the second \( \text{SL}_2(\mathbb{R}) \). Then

\[
\frac{1}{T} \int_X \int_0^T f(xa_{2,t}) \, dt \, d\mu(x).
\]

converges to \( \int_X f \, dm_X \) where \( f \in C_c(X) \) and \( a_{2,t} \in A_2 \) denotes a homomorphism from \( \mathbb{R} \) to \( A_2 \).

Similarly, the above two conjectures can be asked for other quotients for which the analogue of Theorem 2.2 or Theorem 1.4 holds.
References


Applications of Measure Rigidity


[40] Dave Witte Morris, *Ratner’s theorems on unipotent flows*, University of Chicago Press, Chicago, IL (2005), xii+203.


[49] Peter Sarnak, *Recent progress on QUE*.


ETH Zürich, Departement Mathematik
Rämistrasse 101
8092 Zürich
Switzerland
E-mail: manfred.einsiedler@math.ethz.ch