Distribution modulo one and ergodic theory

Jens Marklof

University of Bristol

http://www.maths.bristol.ac.uk

Prospects in Mathematics, Durham, December 2006

Measure rigidity is a branch of ergodic theory that has recently contributed to the solution of some fundamental problems in number theory and mathematical physics. Examples include

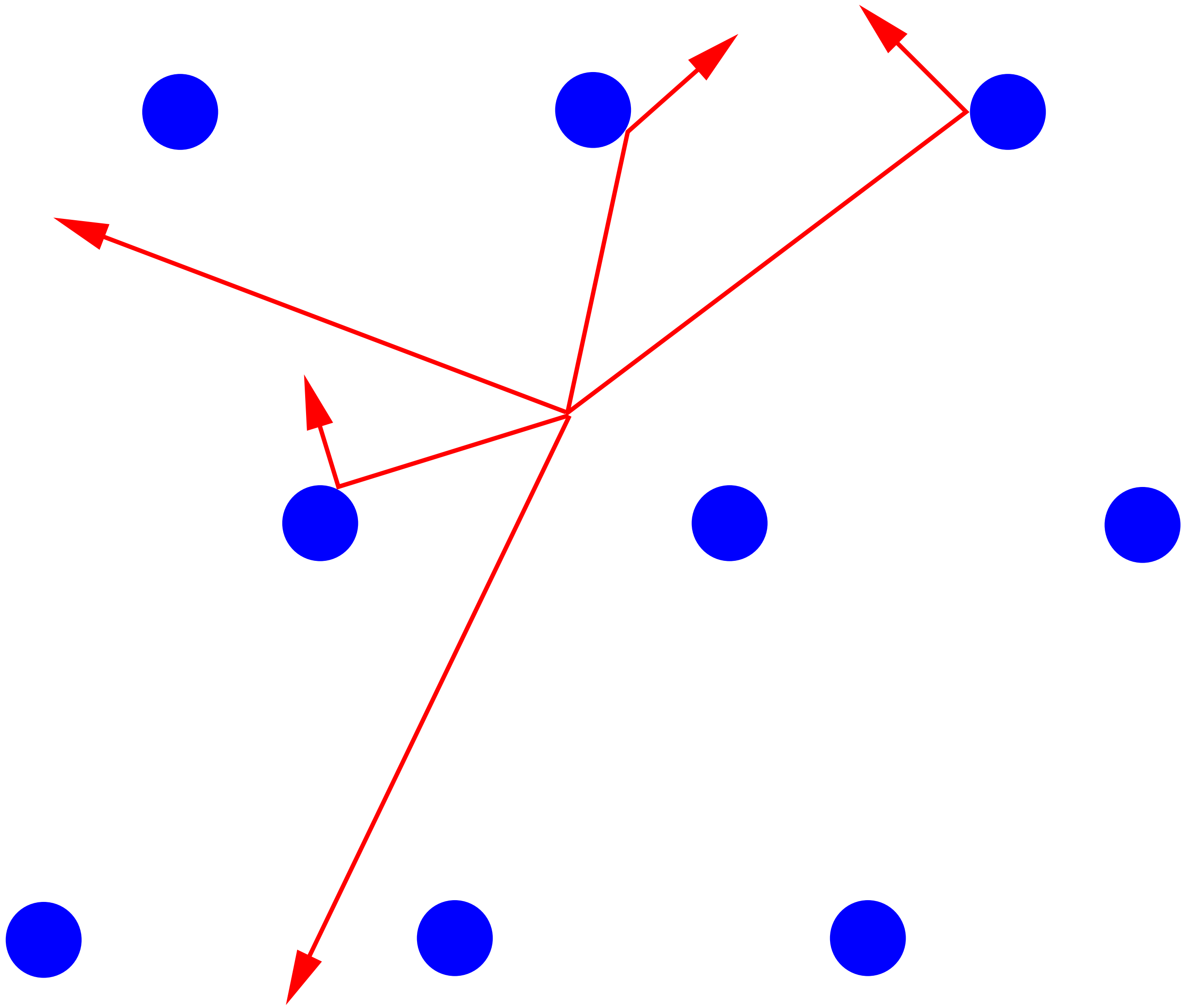
- quantitative versions of the Oppenheim conjecture $m_1^2 + m_2^2 - \sqrt{2}\, m_3^2$
  (Eskin, Margulis & Mozes, Annals of Math 1998)

- spacings between the values of quadratic forms
  $(m_1 - \sqrt{2})^2 + (m_2 - \sqrt{3})^2$ (Marklof, Annals of Math 2003)
  $m_1^2 + \sqrt{2}\, m_2^2$ (Eskin, Margulis & Mozes, Annals of Math 2005)

- quantum unique ergodicity for certain classes of hyperbolic surfaces
  (Lindenstrauss, Annals of Math 2006)

- approach to Littlewood conjecture on the nonexistence of multiplicatively badly approximable numbers
  (Einsiedler, Katok & Lindenstrauss, Annals of Math 2006)

- Boltzmann-Grad limit of the periodic Lorentz gas
  (Marklof & Strömbergsson, in preparation)



Ratner's theorem is one of the central results in measure rigidity. It gives a complete classification of measures invariant under unipotent flows. In this talk I'll discuss a few simple applications of Ratner's theorem to the analysis of the statistical properties of basic number-theoretic sequences:

- fractional parts of $n\alpha$, $n = 1, 2, 3, \ldots$
  (a classical, well understood sequence, usually studied by means of continued fractions; cf. Mazel-Sinai, Bleher, Greenman, Marklof)

- fractional parts of $\sqrt{n\alpha}$, $n = 1, 2, 3, \ldots$
  (as recently studied by Elkies and McMullen, Duke Math J 2004)

- fractional parts of $n^2\alpha$, $n = 1, 2, 3, \ldots$
  (Sinai, Pelegrinotti, Rudnick-Sarnak, Rudnick-Sarnak-Zaharescu, Marklof-Strömbergsson,...)

For more details see

J. Marklof, Distribution modulo one and Ratner's theorem

Proc. Montreal Summer School on Equidistribution in Number Theory 2005 (Springer, to appear)

How to test randomness of point sequences mod 1

Consider an infinite triangular array of numbers on the circle $\mathbb{T} = \mathbb{R}/\mathbb{Z} \simeq [0, 1)$

$$\begin{array}{lllll} \xi_{11} & & & & \\ \xi_{21} & \xi_{22} & & & \\ \vdots & \vdots & \ddots & & \\ \xi_{N1} & \xi_{N2} & \cdots & \xi_{NN} & \\ \vdots & \vdots & & & \ddots \end{array}$$

Assume that each row is ordered, i.e., $\xi_{Nj} \leq \xi_{N(j+1)}$; to simplify notation I'll use ξ_j instead of ξ_{Nj} in the following.

Consider the number of elements in the interval $[x_0 - \frac{\ell}{2}, x_0 + \frac{\ell}{2}) \bmod 1$,

$$S_N(\ell) = \sum_{j=1}^{N} \chi_\ell(\xi_j), \qquad \chi_\ell(x) = \sum_{n\in\mathbb{Z}} \chi_{[-\frac{1}{2},\frac{1}{2})}\left(\frac{x - x_0 + n}{\ell}\right)$$

Here $\chi_{[-\frac{1}{2},\frac{1}{2})}$ denotes the characteristic function of the interval $[-\frac{1}{2}, \frac{1}{2}) \subset \mathbb{R}$.

Uniform distribution mod 1. A sequence $\{\xi_j\}$ is *uniformly distributed mod 1* if for every x_0, ℓ,

$$\lim_{N\to\infty} \frac{S_N(\ell)}{N} = \ell$$

Well known examples of u.d. sequences are $n^k\alpha$ mod 1 ($n = 1, 2, 3, \ldots$), for any $k \in \mathbb{N}$ and α irrational (Weyl 1916)

Poisson distribution. Let $E_N(k,L)$ be the probability of finding k elements in the randomly shifted interval $[x_0, x_0 + \frac{L}{N})$ of size L/N (very small!)

$$E_N(k,L) := \mathrm{meas}\,\{x_0 \in \mathbb{T} : S_N(\ell) = k\}$$

We say the sequence $\{\xi_j\}$ is Poisson distributed if

$$\lim_{N\to\infty} E_N(k,L) = \frac{L^k}{k!}\mathrm{e}^{-L}$$

This means $\{\xi_j\}$ behaves like a generic realization of independent random variables mod 1.

Example. $2^n\alpha \mod 1$ is Poisson distributed for generic α (Rudnick & Zaharescu, Forum Math 2002) and $n^k\alpha \mod 1$ is conjectured to for $k \geq 2$ by some people, others disagree

Distribution of gaps. A popular statistical measure is the distribution of gaps

$$s_j = N(\xi_{j+1} - \xi_j)$$

between consecutive elements. The gap distribution of $\{\xi_j\}$ is

$$P_N(s) = \frac{1}{N} \sum_{j=1}^{N} \delta(s - s_j)$$

and the question is whether it has a limiting distribution

$$P_N(s) \to_w P(s),$$

i.e., for every bounded continuous function $g : \mathbb{R} \to \mathbb{R}$,

$$\lim_{N\to\infty} \int_0^\infty g(s) P_N(s) ds = \int_0^\infty g(s) P(s) ds.$$

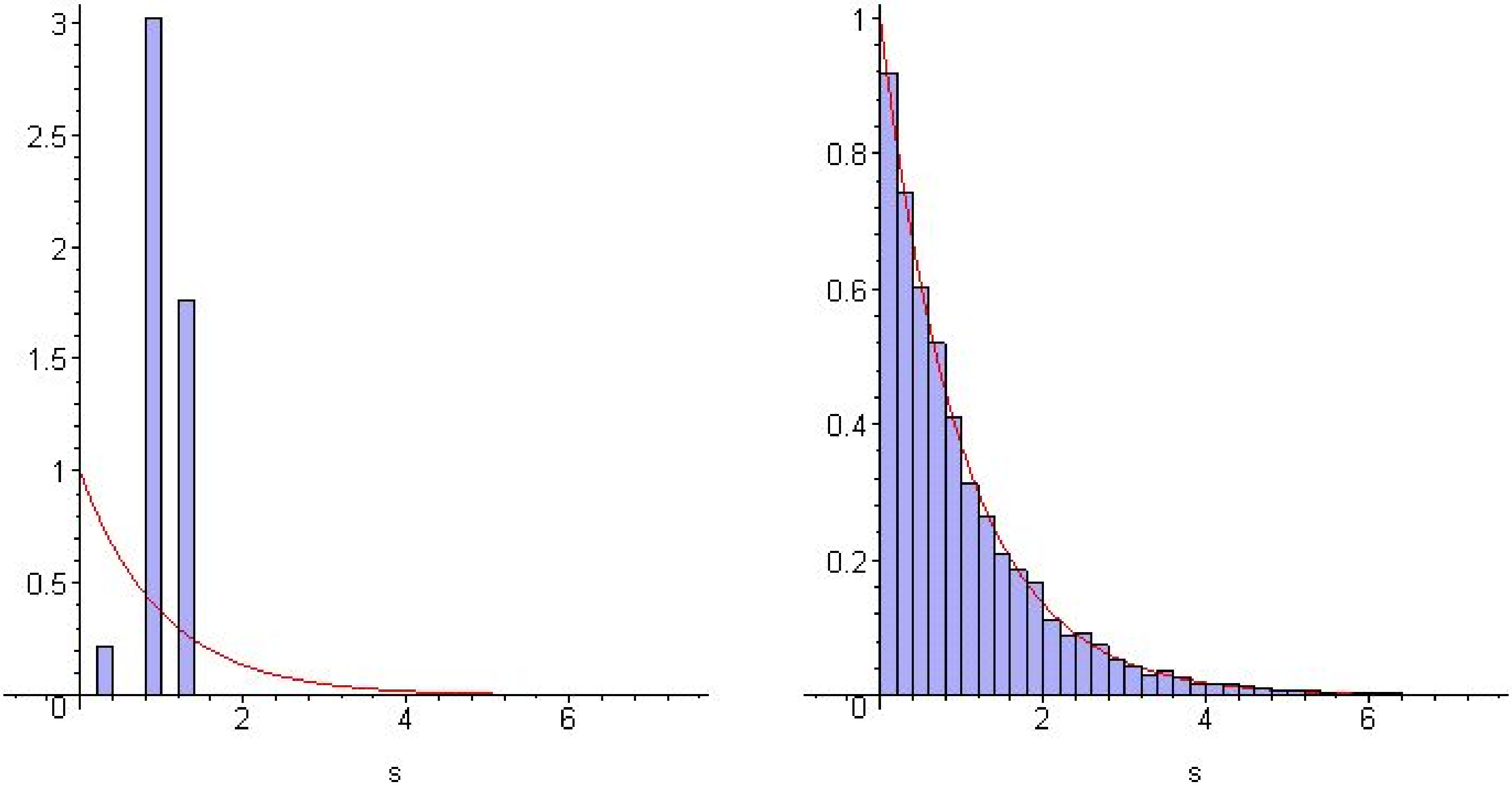
Note one can show

$$P_N(s) \to_w P(s) \iff E_N(0, L) \to E(0, L) \quad \text{with} \quad \frac{d^2 E(0, L)}{dL^2} = P(L)$$

In particular for Poisson distributed sequences $P(s) = \mathrm{e}^{-s}$.

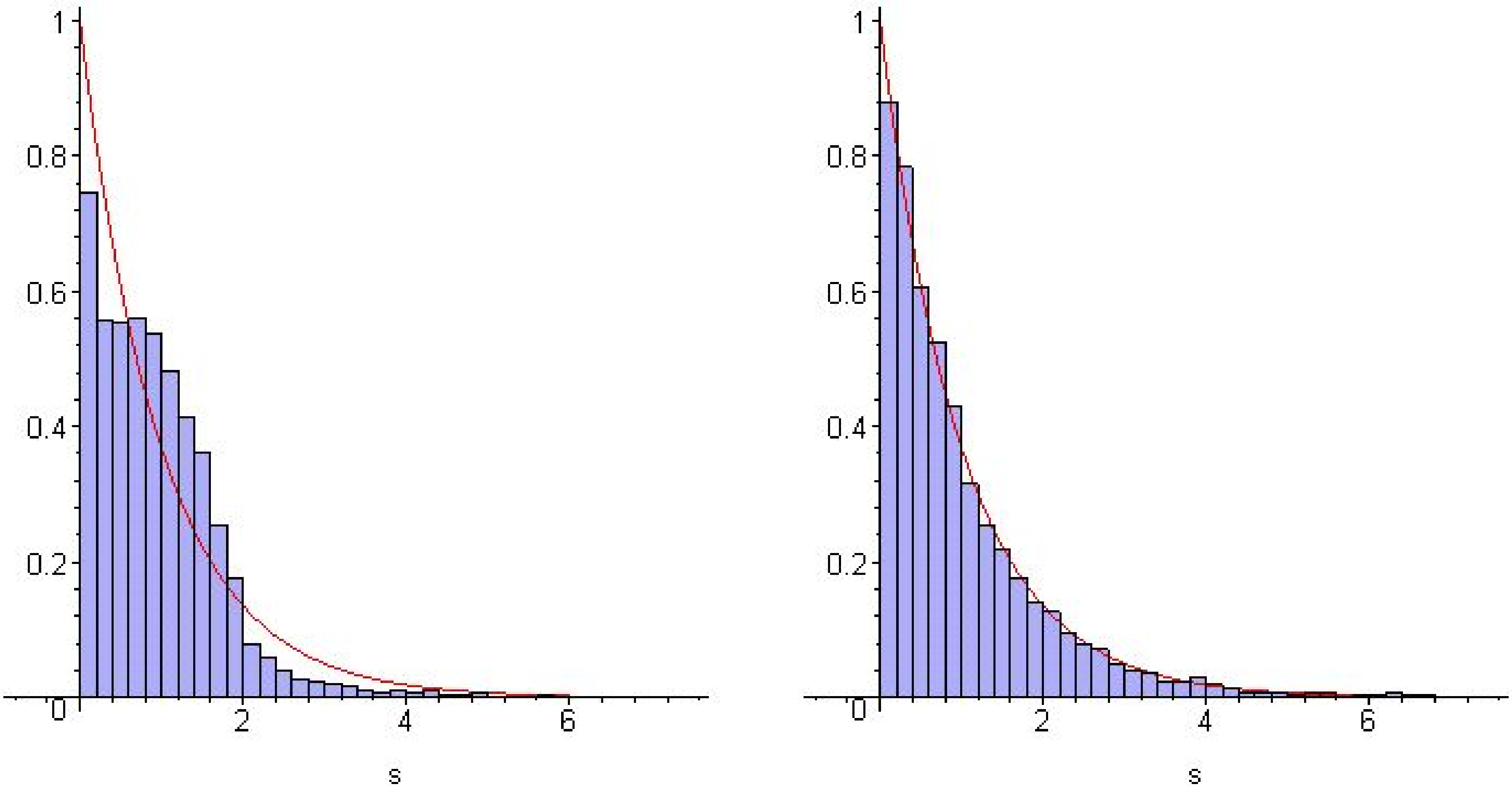
Maple experiments

$P_N(s)$ for $n\sqrt{2}$ and $n^2\sqrt{2}$ vs. the exponential distribution



$N = 6001$

$P_N(s)$ for $\sqrt{n}$ and $\sqrt{n\sqrt{2}}$ vs. the exponential distribution



$N = 10001$

$n\alpha \bmod 1$

The number of elements in an interval of size $\ell = L/N$ and centered at x_0 is

$$
\begin{aligned}
S_N(\ell) &= \sum_{m=1}^{N} \sum_{n\in\mathbb{Z}} \chi_{[-\frac{1}{2},\frac{1}{2})}\left(\frac{N}{L}(m\alpha + n - x_0)\right) \\
&= \sum_{(m,n)\in\mathbb{Z}^2} \chi_{(0,1]}\left(\frac{m}{N}\right)\chi_{[-L/2,L/2]}\big(N(m\alpha + n - x_0)\big) \\
&= \sum_{(m,n)\in\mathbb{Z}^2} \psi\left((m, n - x_0)\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}\begin{pmatrix} N^{-1} & 0 \\ 0 & N \end{pmatrix}\right)
\end{aligned}
$$

where χ_I denotes the characteristic function of the interval $I \subset \mathbb{R}$ and

$$\psi(x,y) = \chi_{(0,1]}(x)\chi_{[-L/2,L/2]}(y)$$

is the characteristic function of a rectangle.

Let $G = \mathrm{SL}(2,\mathbb{R}) \ltimes \mathbb{R}^2$ with multiplication law

$$(M,\xi)(M',\xi') = (MM', \xi M' + \xi'),$$

where $\xi, \xi' \in \mathbb{R}^2$ are viewed as row vectors.

The function

$$F(M,\xi) = \sum_{m\in\mathbb{Z}^2} \psi(mM+\xi)$$

defines a function on G. Note that, with ψ as above, the sum is always finite, and hence F is a piecewise constant function.

Note:

$$S_N(\ell) = F(M,\xi)$$

for

$$M = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} N^{-1} & 0 \\ 0 & N \end{pmatrix}, \qquad \xi = (0, -x_0)M.$$

Homogeneous spaces. The crucial observation is now that F is left-invariant under the discrete subgroup $\Gamma = \mathrm{SL}(2, \mathbb{Z}) \ltimes \mathbb{Z}^2$

$$F(\gamma g) = F(g) \qquad \forall \quad \gamma \in \Gamma$$

(this can be checked by an elementary calculation), and hence F may be viewed as a piecewise constant function on the homogeneous space $\Gamma \backslash G$.

Dynamics on $\Gamma\backslash G$. Right multiplication by

$$\Phi^t = \left(\begin{pmatrix} \mathrm{e}^{-t/2} & 0 \\ 0 & \mathrm{e}^{t/2} \end{pmatrix}, 0 \right)$$

genrates a flow on $\Gamma\backslash G$

$$\Gamma g \mapsto \Gamma g \Phi^t.$$

Now observe that $S_N(\ell)$ is related to a function F on $\Gamma\backslash G$ evaluated along an orbit of this flow:

$$S_N(\ell) = F(g_0 \Phi^t)$$

with $t = 2 \log N$ and initial condition

$$g_0 = g_0(\alpha, x_0) = \left(\begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}, (0, -x_0) \right)$$

Equidistribution

Theorem. *For any bounded, piecewise continuous* $f : \Gamma\backslash G \to \mathbb{R}$

$$\lim_{t\to\infty} \frac{1}{b-a} \int_a^b \int_0^1 f(g_0(\alpha, y)\Phi^t) d\alpha\, dy = \frac{1}{\mu(\Gamma\backslash G)} \int_{\Gamma\backslash G} f\, d\mu.$$

This theorem can be proved by exploiting the mixing property of the flow Φ^t. By chosing the right test function f, the following theorem (first proved by Mazel-Sinai, and for $P(s)$ by Bleher using different methods based on cont'd fractions) is a direct corollary.

Values of $n\alpha$ in short intervals for random α

Theorem. *For any* $L > 0$,

$$\lim_{N\to\infty} \frac{\text{meas}\{(\alpha, x_0) \in [a, b] \times [0, 1] : S_N(\ell) = k\}}{b-a} = E(k, L),$$

where

$$E(k, L) = \frac{\mu(g \in \Gamma\backslash G : F(g) = k)}{\mu(\Gamma\backslash G)}.$$

Equidistribution II. Using Ratner's theorem, one can in fact strengthen the previous results by showing:

Theorem. *For any irrational* x_0 *and any bounded, piecewise continuous* $f : \Gamma\backslash G \to \mathbb{R}$

$$\lim_{t\to\infty} \frac{1}{b-a} \int_a^b f(g_0(\alpha, x_0)\Phi^t)\, d\alpha = \frac{1}{\mu(\Gamma\backslash G)} \int_{\Gamma\backslash G} f\, d\mu.$$

(Remarkably, A. Strömbergsson has recently proved this results by analytic techniques, without using Ratner's theory.)

Hence we obtain the value distribution in intervals with fixed rather than random x_0.

Theorem. *For any* $L > 0$ *and* x_0 *irrational,*

$$\lim_{N\to\infty} \frac{\text{meas}\{\alpha \in [a,b] : S_N(\ell) = k\}}{b-a} = E(k, L),$$

with the same $E(k, L)$ *as before.*

$$\sqrt{n\alpha} \bmod 1$$

We are interested in the distribution of

$$S_N(\ell) = \sum_{n=1}^{N} \sum_{m \in \mathbb{Z}} \chi_{[-\frac{1}{2},\frac{1}{2})} \left(\frac{N}{L} (\sqrt{n\alpha} - x_0 + m) \right).$$

Similar to the previous section on can show that for $\boldsymbol{\alpha = 1}$

$$S_N(\ell) \approx F(g_0(x)\Phi^t)$$

with $t = 2 \log N$ and initial condition

$$g_0(x) = \left(\begin{pmatrix} 1 & 2x \\ 0 & 1 \end{pmatrix}, (x, x^2) \right)$$

Again

$$F(M, \xi) = \sum_{m \in \mathbb{Z}^2} \psi(mM + \xi)$$

but now

$$\psi(x, y) = \chi_{(0,1]}(x) \chi_{(-L,L]} \left(\frac{y}{x} \right)$$

which represents the characteristic function of a triangle.

Equidistribution III

The following follows again from Ratner's theorem (Elkies & McMullen 2004).

Theorem. *For any bounded, piecewise continuous* $f : \Gamma\backslash G \to \mathbb{R}$

$$\lim_{t\to\infty} \int_0^1 f(g_0(x)\Phi^t)\, dx = \frac{1}{\mu(\Gamma\backslash G)} \int_{\Gamma\backslash G} f\, d\mu.$$

This implies, as before:

Values of $\sqrt{n}$ in short intervals

Theorem. *For any* $L > 0$*,*

$$\lim_{N\to\infty} \mathrm{meas}\{x \in [0,1] : S_N(\ell) = k\} = E(k,L),$$

where

$$E(k,L) = \frac{\mu(g \in \Gamma\backslash G : F(g) = k)}{\mu(\Gamma\backslash G)}.$$

The above argument can be adapted for rational α but no longer works for irrational α. In fact heuristic arguments (see lecture notes) as well as numerical experiments predict that then $\sqrt{n\alpha}$ should be Poisson distributed, at least for typical α.

Ratner’s theorem

Let

— G be a Lie group (e.g. $\mathrm{SL}(2,\mathbb{R}) \ltimes \mathbb{R}^2$)

— Γ be a discrete subgroup (e.g. $\mathrm{SL}(2,\mathbb{Z}) \ltimes \mathbb{Z}^2$)

— U a group generated by unipotent subgroups

Examples of such U we had discussed earlier are

$$\left\{\left(\begin{pmatrix}1 & t\\ 0 & 1\end{pmatrix}, 0\right)\right\}_t \qquad \left\{\left(\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}, (0,t)\right)\right\}_t \qquad \left\{\left(\begin{pmatrix}1 & 2t\\ 0 & 1\end{pmatrix}, (t,t^2)\right)\right\}_t$$

Ratner's theorem. *Let ν be an ergodic, right-U-invariant probability measure on $\Gamma\backslash G$. Then there is a closed, connected subgroup $H \subset G$, and a point $\overline{g} \in \Gamma\backslash G$ such that*

1. *ν is H-invariant,*

2. *ν is supported on the orbit $\overline{g}H$.*

Equidistribution IV

The equidistribution theorems we had used earlier are corollaries of the following theorem, which in turn is a special case of a theorem by Shah (Proc. Indian Acad Sci 1996).

Theorem. *Suppose G contains a Lie subgroup H isomorphic to $\mathrm{SL}(2,\mathbb{R})$ (we denote the corresponding embedding by $\varphi : \mathrm{SL}(2,\mathbb{R}) \to G$), such that the set $\Gamma\backslash\Gamma H$ is dense in $\Gamma\backslash G$. Then, for any bounded continuous $f : \Gamma\backslash G \to \mathbb{R}$*

$$\lim_{t\to\infty} \int_a^b f\left(\varphi\left(\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}\begin{pmatrix} \mathrm{e}^{-t/2} & 0 \\ 0 & \mathrm{e}^{t/2} \end{pmatrix}\right)\right) dx = \frac{b-a}{\mu(\Gamma\backslash G)} \int_{\Gamma\backslash G} f d\mu$$

where μ is the Haar measure of G.

The general strategy of proof for statements of the above type is as follows.

1. Show that the sequences of probability measures ν_t defined by

$$\nu_t(f) = \frac{1}{b-a}\int_a^b f\left(\varphi\left(\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\begin{pmatrix}e^{-t/2} & 0\\ 0 & e^{t/2}\end{pmatrix}\right)\right)dx$$

is tight. Then, by the Helly-Prokhorov theorem, it is relatively compact, i.e., every sequence of ν_t contains a convergent subsequence with weak limit ν, say.

3. Show that ν is invariant under a unipotent subgroup U; in the present case,

$$U = \left\{\varphi\left(\begin{pmatrix}1 & x\\ 0 & 1\end{pmatrix}\right)\right\}_{x\in\mathbb{R}}.$$

4. Use a density argument to rule out measures concentrated on subvarieties (exploit the assumption that $\Gamma\backslash\Gamma H$ is dense in $\Gamma\backslash G$).