Random lattices and their applications in number theory, geometry and statistical mechanics II

Jens Marklof
University of Bristol

Tata Institute for Fundamental Research, Mumbai, February 2023

Outline

Lecture 1 What are random lattices? Basic features and examples

Lecture 2 Random lattices in number theory and geometry

Lecture 3 Random lattices in statistical mechanics – the Lorentz gas

Randomness mod 1

Consider a sequence of real numbers $(\xi_n)_n$ mod 1, and for $\xi_1, \dots, \xi_N$ denote by $s_1, \dots, s_N$ the N gaps between consecutive $\xi_j \bmod 1$.

Gap distribution:

$$P_N(L) := \frac{\#\{n \le N : s_n > \frac{L}{N}\}}{N}$$

Two point correlation:

$$R_N(a, b) := \frac{\#\{(m, n) : m \ne n \le N,\ \xi_m - \xi_n \in [\frac{a}{N}, \frac{b}{N}] + \mathbb{Z}\}}{N}$$

Theorem A. Let (ξ_n) be an iid sequence, uniformly distributed mod 1. Then Lebesgue-a.s.

$$\lim_{N\to\infty} P_N(L) = \int_L^\infty \mathrm{e}^{-s} ds, \qquad \lim_{N\to\infty} R_N(a,b) = b - a$$

"Gap and two-point statistics are Poisson"

Random matrices

Theorem B. (Wigner 1950s, Gaudin 1961)
Let $(\xi_n)_{n\leq N}$ the ev's of $A \in U(N)$. Then Haar-a.s.

$$\lim_{N\to\infty} P_N(L) = P_{\mathrm{Gaudin}}(L), \qquad \lim_{N\to\infty} R_N(a,b) = \int_a^b \left(1 - \left(\frac{\sin(\pi s)}{\pi s}\right)^2\right) ds$$

- $P_{\mathrm{Gaudin}}(L)$ is given by Painlevé transcendent

- Wigner surmise:

$$P_{\mathrm{Gaudin}}(L) \approx \int_L^\infty \frac{32}{\pi^2} s^2 \mathrm{e}^{-4s^2/\pi} ds$$

Riemann zeros

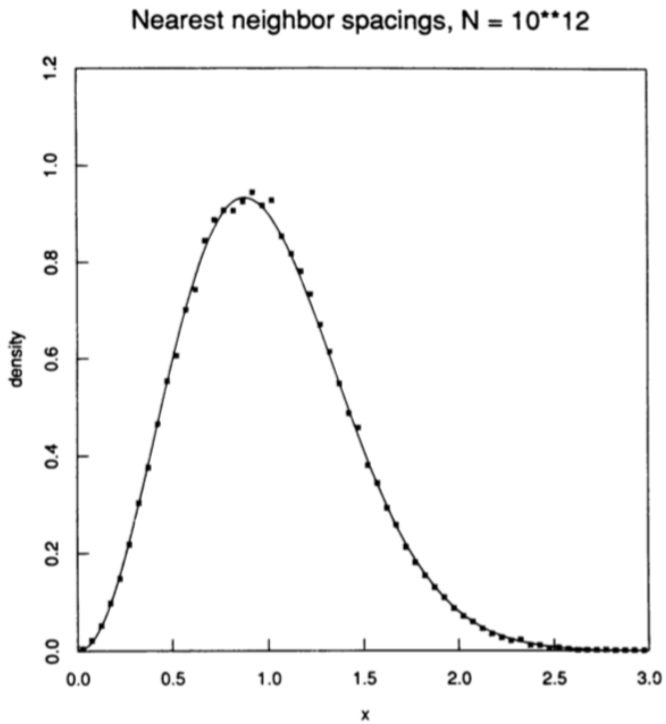


FIGURE 4

Probability density of the normalized spacings δ_n. Solid line: GUE prediction. Scatter plot: empirical data based on zeros γ_n, $10^{12} + 1 \leqslant n \leqslant 10^{12} + 10^5$.

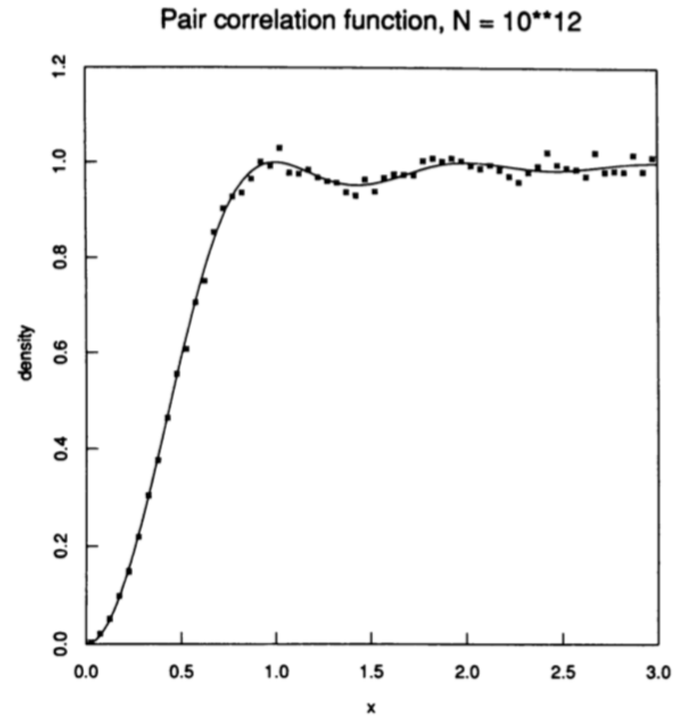


FIGURE 2

Pair correlation of zeros of the zeta function. Solid line: GUE prediction. Scatter plot: empirical data based on zeros γ_n, $10^{12} + 1 \leqslant n \leqslant 10^{12} + 10^5$.

A. M. Odlyzko, Math. Comp., 48 (1987), pp. 273-308

Lacunary sequences

Theorem C. (Rudnick & Zaharescu, Forum Math 2002)
Let $\xi_n = a_n\alpha \bmod 1$ with (a_n) an integer lacunary sequence (i.e. $\liminf \frac{a_{n+1}}{a_n} > 1$). Then for Lebesgue-a.e. α,

$$\lim_{N\to\infty} P_N(L) = \int_L^\infty \mathrm{e}^{-s} ds, \qquad \lim_{N\to\infty} R_N(a,b) = b-a$$

- Proof for all k-point correlation functions
- Fourier analysis in α reduces problem to estimates of number of solutions of exponential Diophantine equations
- $a_n = 2^n$ gives Poisson limit law for typical orbit of the "chaotic" doubling map $\alpha \mapsto 2\alpha \bmod 1$

Polynomials mod 1

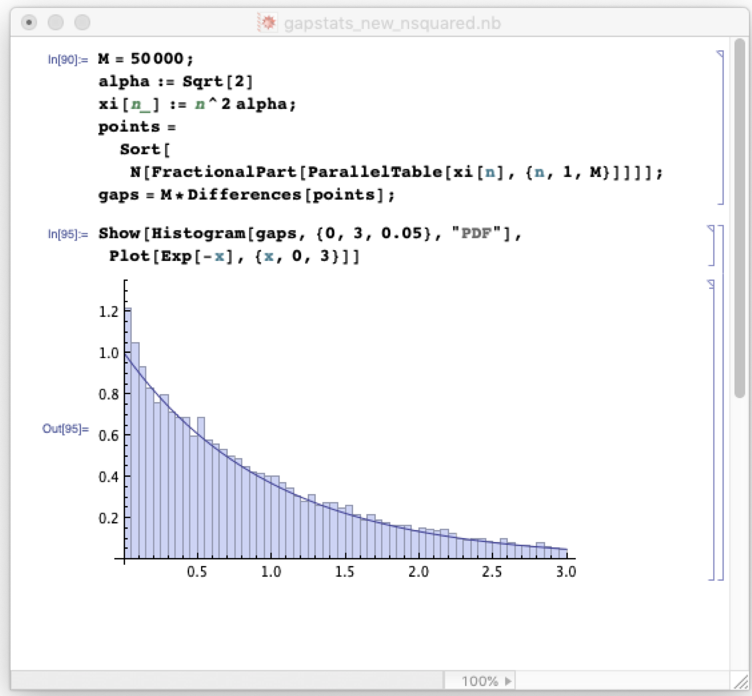
Theorem D. (Rudnick & Sarnak, Comm Math Phys 1998)
Let $\xi_n = n^k\alpha \bmod 1$, with fixed integer $k \geq 2$. Then for Lebesgue a.e. α,

$$\lim_{N\to\infty} R_N(a,b) = b - a$$

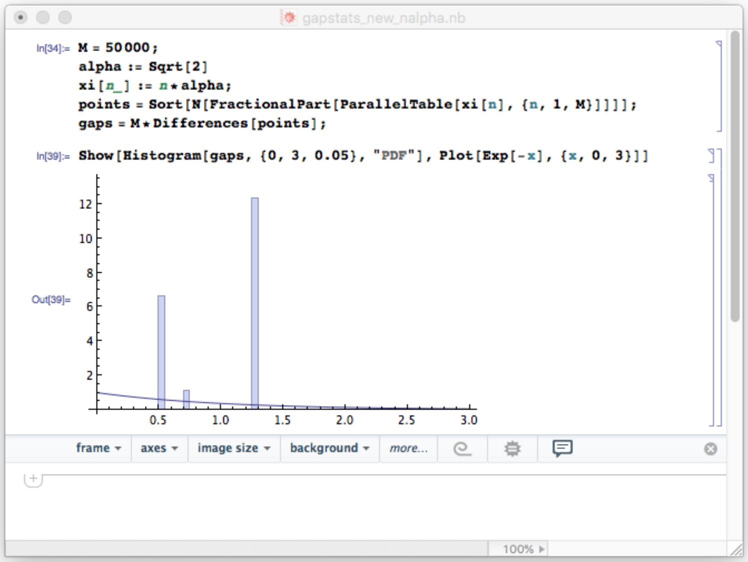
- Proof uses averages over Weyl sums and estimating solutions to polynomial Diophantine equations

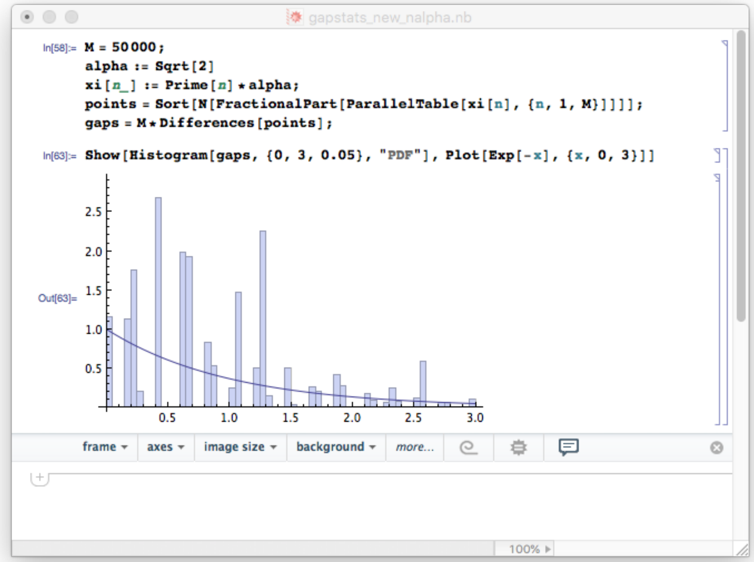
- Rudnick, Sarnak & Zaharescu: for α that are well-approximable by rationals, proof of convergence of gap distribution P_N for $n^2\alpha$ to exponential distribution **along subsequence of** N; for these however convergence not expected along full sequence

- **No proofs for P_N, nor for R_N for explicit examples of α** e.g. for $\alpha = \sqrt{2}$; cf. algorithmic characterization by Heath-Brown (Math Proc Camb Phil Soc 2010).



Linear polynomials mod 1





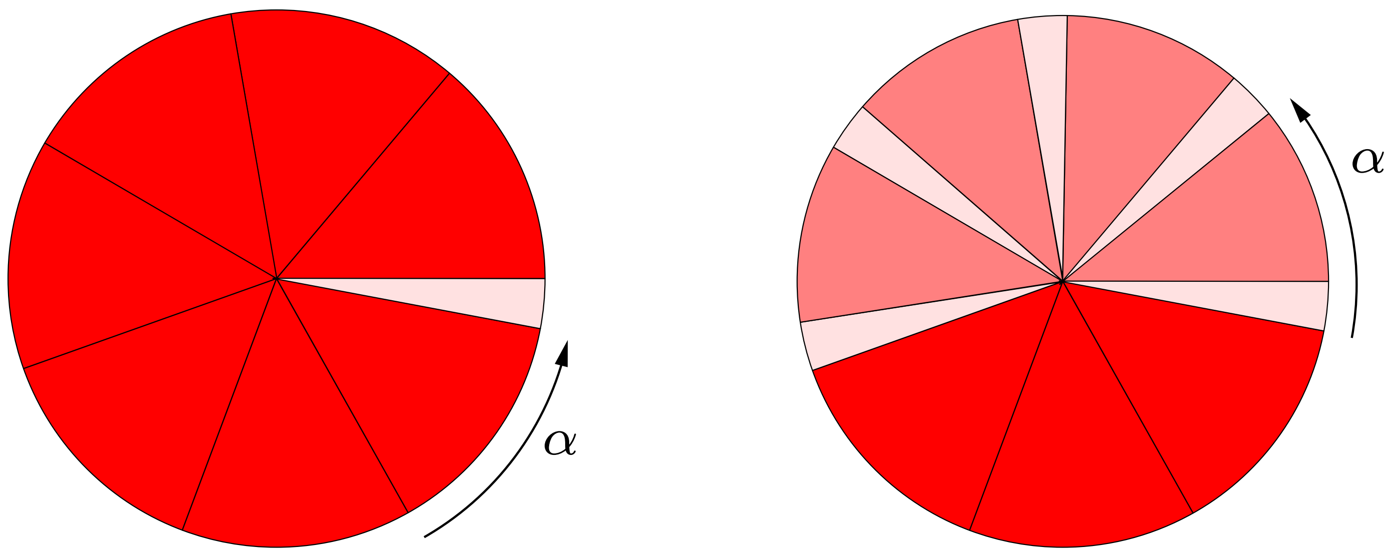
The gap and two-point statistics of $\xi_n = n\alpha \bmod 1$ do not converge for $\alpha \notin \mathbb{Q}$ (three gap theorem*), but will after randomizing α or N (Bleher 1990-92, Mazel & Sinai 1992, Greenman 1996, Marklof ETDS 2000).

Not much is known about $\xi_n = p_n\alpha \bmod 1$ with p_n the nth prime, except that the two-point statistics do not converge (Walker, Mathematika 2018).

[*see M. & Strömbergsson, American Math Monthly 2018]

The three gap theorem (Steinhaus conjecture)

“There are at most three distinct gap lengths in the fractional parts of the sequence $\alpha, 2\alpha, \ldots, N\alpha$*, for any integer* N *and real number* α*.”*



Sós (1957), Surányi (1958), Świerczkowski (1959)

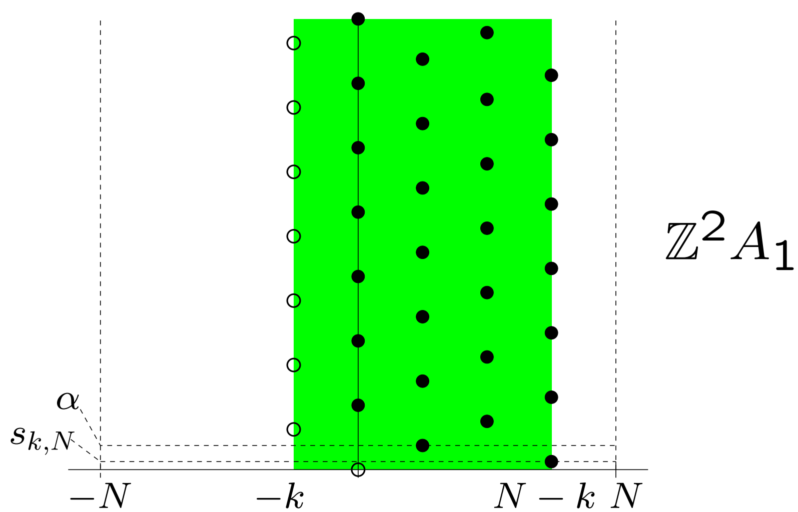
The three gap theorem and the space of lattices

JM & Strömbergsson, American Math. Monthly 2017

The gap between $\xi_k = k\alpha \bmod 1$ and its *next* neighbour on $\mathbb{R}/\mathbb{Z}$ is given by

$$\begin{aligned} s_{k,N} &= \min\{(\ell-k)\alpha + n > 0 \mid (\ell,n)\in\mathbb{Z}^2,\ 0<\ell\le N\} \\ &= \min\{m\alpha + n > 0 \mid (m,n)\in\mathbb{Z}^2,\ -k<m\le N-k\} \\ &= \min\{y>0 \mid (x,y)\in\mathbb{Z}^2 A_1,\ -k<x\le N-k\}, \end{aligned}$$

with the matrix $A_1 = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$.



An $\mathsf{SL}(2,\mathbb{Z})$-invariant function

Set $G = \mathsf{SL}(2,\mathbb{R})$, $\Gamma = \mathsf{SL}(2,\mathbb{Z})$.

For $M \in G$, $0 < t \le 1$, define

$$F(M,t) = \min\left\{ y > 0 \,\middle|\, (x,y) \in \mathbb{Z}^2 M,\ -t < x \le 1-t \right\}.$$

Key point:

$$\begin{aligned} s_{k,N} &= \frac{1}{N} \min\left\{ y > 0 \,\middle|\, (x,y) \in \mathbb{Z}^2 A_N(\alpha),\ -\frac{k}{N} < x \le 1-\frac{k}{N} \right\} \\ &= \frac{1}{N} F\left(A_N(\alpha), \frac{k}{N} \right) \end{aligned}$$

with $A_N(\alpha) = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} \begin{pmatrix} N^{-1} & 0 \\ 0 & N \end{pmatrix} \in G$

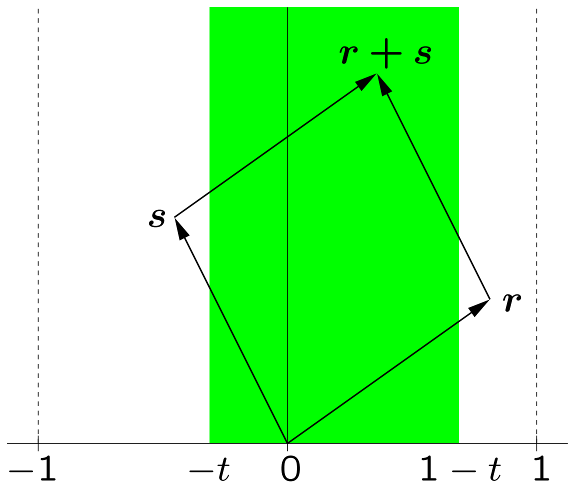
An $\mathrm{SL}(2,\mathbb{Z})$-invariant function

$$F(M,t) = \min\left\{y > 0 \;\middle|\; (x,y) \in \mathbb{Z}^2 M,\ -t < x \le 1-t\right\}.$$

Proposition 1. F is well-defined as a function $\Gamma\backslash G \times (0,1] \to \mathbb{R}_{>0}$.

Proposition 2. For every given $M \in G$, the function $t \mapsto F(M,t)$ is piecewise constant and takes at most three distinct values. If there are three values, then the third is the sum of the first and second.

Proof:



Gap distribution

$$P_N(L) := \frac{\#\{k \le N : s_{k,N} > \frac{L}{N}\}}{N} = \frac{\#\{k \le N : F(A_N(\alpha), \frac{k}{N}) > L\}}{N}$$

For N large,

$$P_N(L) \sim \text{meas}\{t \in [0,1] : F(A_N(\alpha), t) > L\}$$

Since the function $M \mapsto \text{meas}\{t \in [0,1] : F(M,t) > L\}$ is a non-trivial function on $\Gamma\backslash G$, the limit $\lim_{N\to\infty} P_N(L)$ will not exist.

However, if we consider α random (w.r.t. an a.c. λ), then

$$\lim_{N\to\infty} \int_0^1 P_N(L)\lambda(d\alpha) = \int_{\Gamma\backslash G} \int_0^1 \mathbf{1}[F(M,t) > L]\, dt\, d\mu_0(M) =: P(L).$$

This follows from the equidistribution of long closed horocycles: for any bounded continuous $f : \Gamma\backslash G \to \mathbb{R}$, λ Borel a.c. prob. meas.,

$$\lim_{N\to\infty} \int_0^1 f(A_N(\alpha))\lambda(d\alpha) = \int_{\Gamma\backslash G} f(M) d\mu_0(M).$$

How to compute $P(L)$

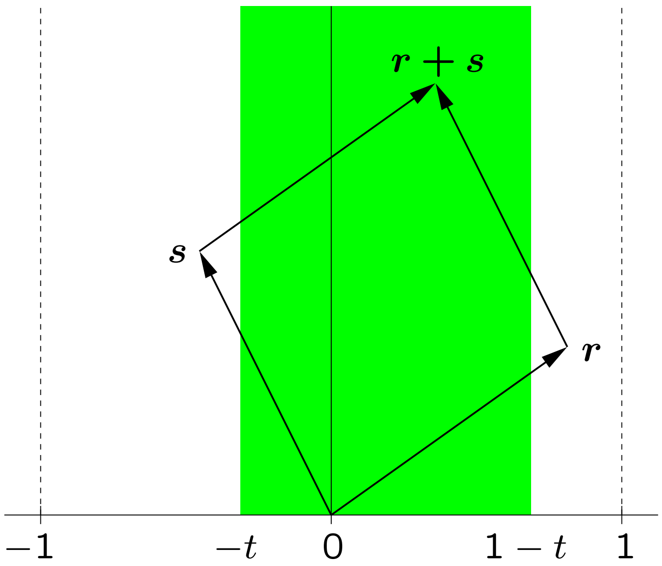
We need to work out the distribution of the lowest height vector inside the green strip.

The trick is to disintegrate. Recall the "space of random lattices"

$$X = \Gamma \backslash G, \quad G = \mathrm{SL}(2, \mathbb{R}), \quad \Gamma = \mathrm{SL}(2, \mathbb{Z})$$

Now for each non-zero $\boldsymbol{y} \in \mathbb{R}^2$ consider the subspace

$$X(\boldsymbol{y}) = \{\Gamma M \in X : \boldsymbol{y} \in \mathbb{Z}^2 M\}$$



To determine the restriction to $X(\boldsymbol{y})$ of the Haar probability measure μ on X we further decompose

$$X(\boldsymbol{y}) = \bigcup_{\boldsymbol{k}\in\mathbb{Z}^2\setminus\{0\}} X(\boldsymbol{k},\boldsymbol{y}), \quad X(\boldsymbol{k},\boldsymbol{y}) = \{\Gamma M : M \in G,\ \boldsymbol{k}M = \boldsymbol{y}\}$$

For every $\boldsymbol{k} = (k_1, k_2)$ with $\gcd(k_1, k_2) = r$ we find $\gamma \in \Gamma$ such that

$$r\boldsymbol{e}_1\gamma = \boldsymbol{k}, \qquad \boldsymbol{e}_1 = (1, 0)$$

. This yields the disjoint union

$$X(\boldsymbol{y}) = \bigcup_{r=1}^{\infty} X(r\boldsymbol{e}_1,\boldsymbol{y}), \qquad X(r\boldsymbol{e}_1,\boldsymbol{y}) = \{\Gamma M : M \in G,\ r\boldsymbol{e}_1 M = \boldsymbol{y}\}$$

Take $M_{\boldsymbol{y}}$ such that $\boldsymbol{y} = \boldsymbol{e}_1 M_{\boldsymbol{y}}$ (e.g. $M_y = \begin{pmatrix} y_1 & y_2 \\ -y_2^{-1} & 0 \end{pmatrix}$ for $y_2 > 0$), and note that

$$\boldsymbol{e}_1 M = \boldsymbol{e}_1 \text{ for all } M \in H, \qquad H := \left\{ \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix} : v \in \mathbb{R} \right\}$$

Set $a(r) = \begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix}$. Then

$$\begin{aligned} X(r\boldsymbol{e}_1, \boldsymbol{y}) &= \{\Gamma M : M \in G,\ r\boldsymbol{e}_1 M = \boldsymbol{e}_1 M_{\boldsymbol{y}}\} \\ &= \{\Gamma M : M \in G,\ \boldsymbol{e}_1 a(r) M = \boldsymbol{e}_1 M_{\boldsymbol{y}}\} \\ &= \{\Gamma a(r)^{-1} h M_{\boldsymbol{y}} : h \in H\} \\ &= a(r)^{-1}\{\tilde{\Gamma} h M_{\boldsymbol{y}} : h \in H\} \end{aligned}$$

where $\tilde{\Gamma} := a(r)\Gamma a(r)^{-1}$ and

$$\begin{aligned} \{\tilde{\Gamma} h M_{\boldsymbol{y}} : h \in H\} &= \tilde{\Gamma}\backslash\tilde{\Gamma} H M_{\boldsymbol{y}} \\ &\simeq \tilde{\Gamma}_\infty \backslash H M_{\boldsymbol{y}} \end{aligned}$$

$$\tilde{\Gamma}_\infty = a(r)\left\{ \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix} : m \in \mathbb{Z} \right\} a(r)^{-1} = \left\{ \begin{pmatrix} 1 & 0 \\ r^{-2} m & 1 \end{pmatrix} : m \in \mathbb{Z} \right\}$$

The Haar probability measure on

$$X(\boldsymbol{y}) = \bigcup_{r=1}^{\infty} a(r)^{-1}\{\tilde{\Gamma} h M_{\boldsymbol{y}} : h \in H\}$$

is thus

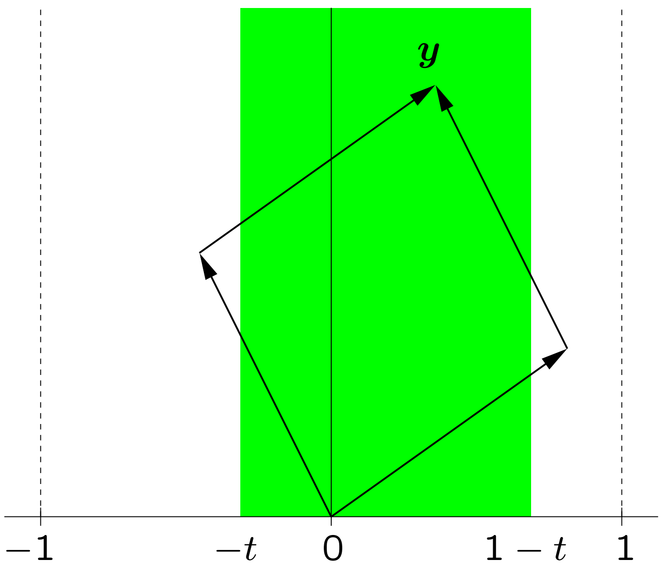
$$\left(\sum_{r=1}^{\infty} r^{-2}\right)^{-1} dv = \frac{6}{\pi^2}\, dv$$

The Haar probability measure on X reads then (recall that $\boldsymbol{y}$ ranges over a unit volume)

$$\mu = \frac{6}{\pi^2}\, dv\, dy_1\, dy_2$$

We now want to work out that, given $\boldsymbol{y}$ in the green strip, the measure of v such that there is no other vector of smaller height in the green strip.

Now, $X(r\boldsymbol{e}_1, \boldsymbol{y})$ corresponds to a lattice $\mathbb{Z}^2 M$ where $r(1,0)M = \boldsymbol{y}$, so the top row of M equals $r^{-1}\boldsymbol{y}$. This means that $r^{-1}\boldsymbol{y} \in \mathbb{Z}^2 M$ and, for $k \geq 2$, is a vector in the green strip (since $\boldsymbol{y}$ is) but of smaller height than $\boldsymbol{y}$ - these are excluded. We therefore only need to integrate over $X(\boldsymbol{e}_1, \boldsymbol{y})$ rather than the full $X(\boldsymbol{y})$.

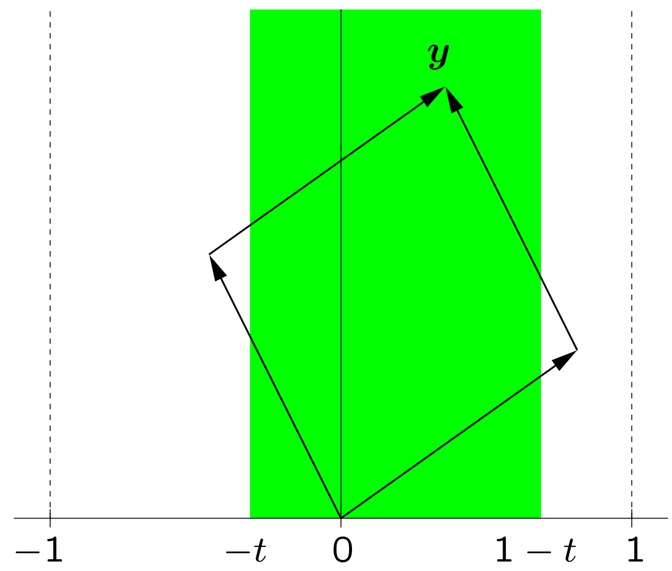


This is now a simple integral over $v \in [0,1]$ with the condition that the lattice

$$\mathbb{Z}^2 \begin{pmatrix} 1 & 0 \\ v & 1 \end{pmatrix} \begin{pmatrix} y_1 & y_2 \\ -y_2^{-1} & 0 \end{pmatrix}$$

has no lattice point in the green strip below $\boldsymbol{y}$.

This can be calculated by distinguishing the three cases for $\boldsymbol{y}$ being basis vectors (or their linear combination) as in the diagram, and we obtain:



$$K_w(\boldsymbol{y}) = \frac{6}{\pi^2} \, H\left(1 + \frac{y_2^{-1} - \max\left(|w|, |y_1 - w|\right) - \frac{1}{2}}{|y_1|} \right)$$

where $w = \frac{1}{2} - t$ is the center of the interval $[-t, 1-t]$ and

$$H(x) = \begin{cases} 0 & \text{if } x \leq 0 \\ x & \text{if } 0 < x < 1 \\ 1 & \text{if } 1 \leq x. \end{cases}$$

JM & Strömbergsson, Nonlinearity 2008

Nearest neighbours in Kronecker sequences

- Fix $\vec{\alpha} \in \mathbb{R}^d$, multidimensional torus $\mathbb{T}^d = \mathbb{R}^d/\mathbb{Z}^d$

- Consider distances between points $\xi_n = n\vec{\alpha} \in \mathbb{T}^d$, $n = 1, \ldots, N$

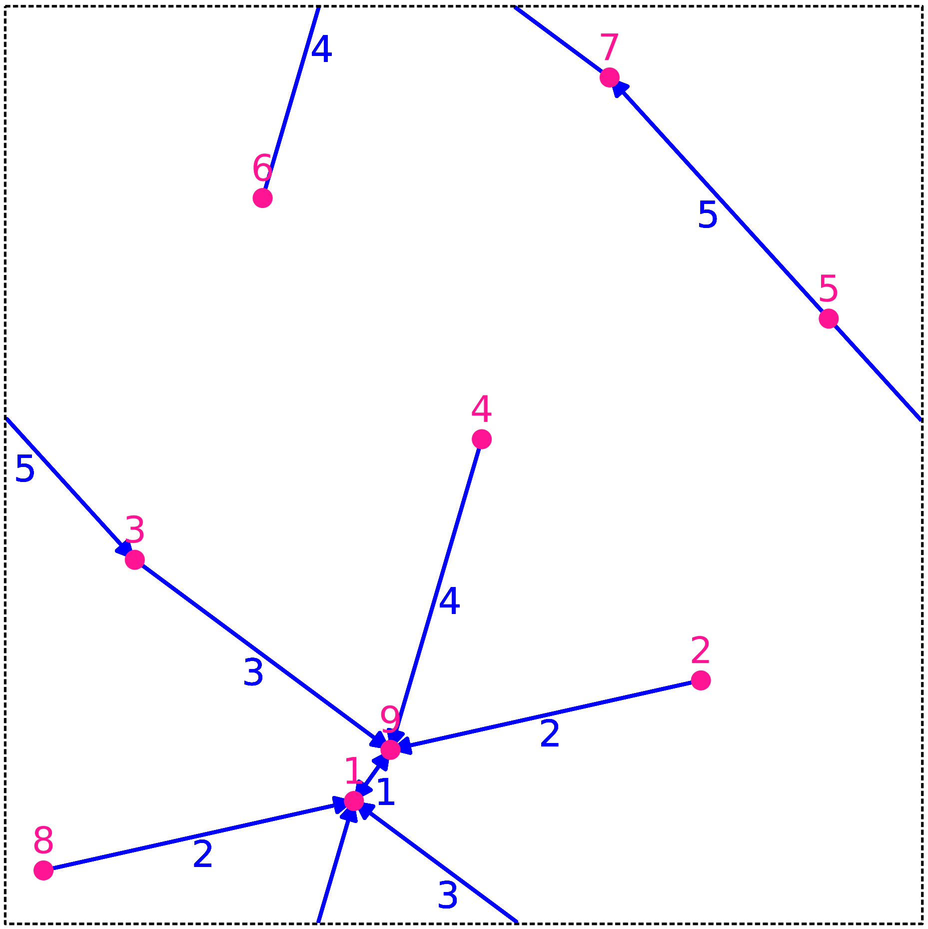
- $\delta_{n,N} = \min\{|\xi_m - \xi_n + \ell| > 0 \mid 1 \leq m \leq N,\ \ell \in \mathbb{Z}^d\}$

  (= distance of ξ_n to its nearest neighbour, $|\cdot|$ denotes Euclidean norm in $\mathbb{R}^d$)

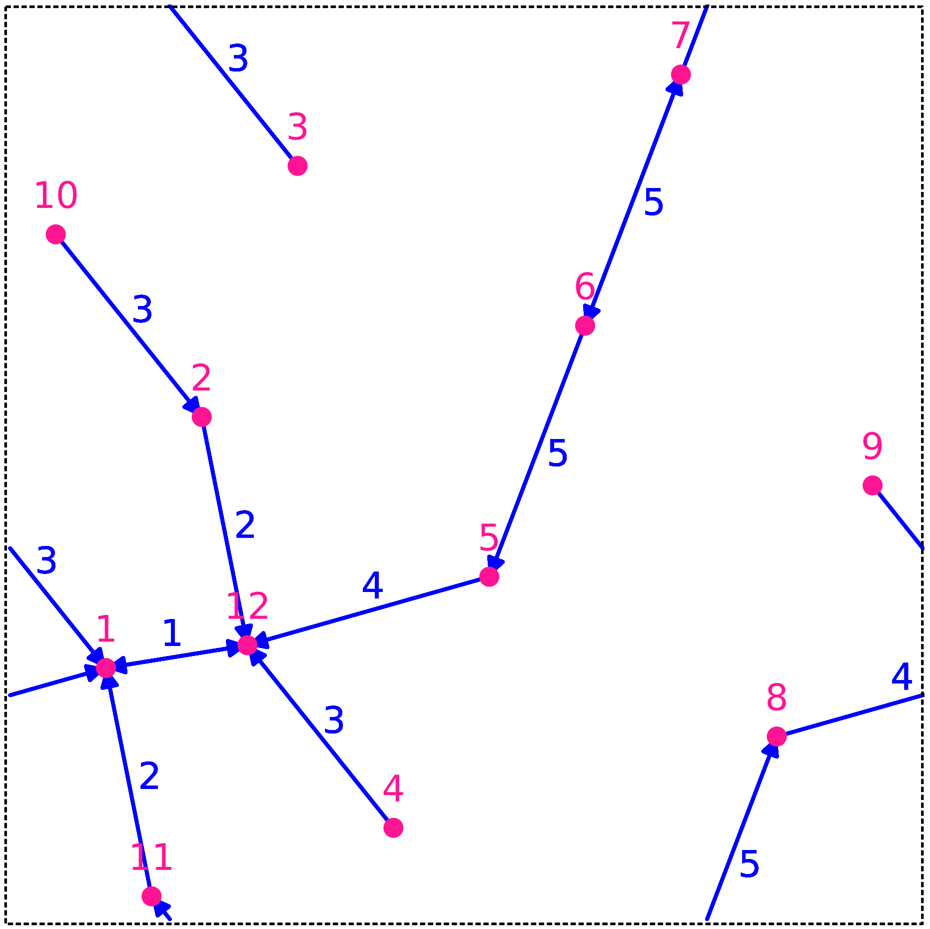
- Number of distinct distances $g_N = |\{\delta_{n,N} \mid 1 \leq n \leq N\}|$

- Previous studies by Chevallier (1996, 1997, 2000, 2014) and Vijay (2008, “11 distances are enough”; see also Biringer and Schmidt for actions by isometries on general compact manifolds (2008)

Examples with 5 distances in dimension 2

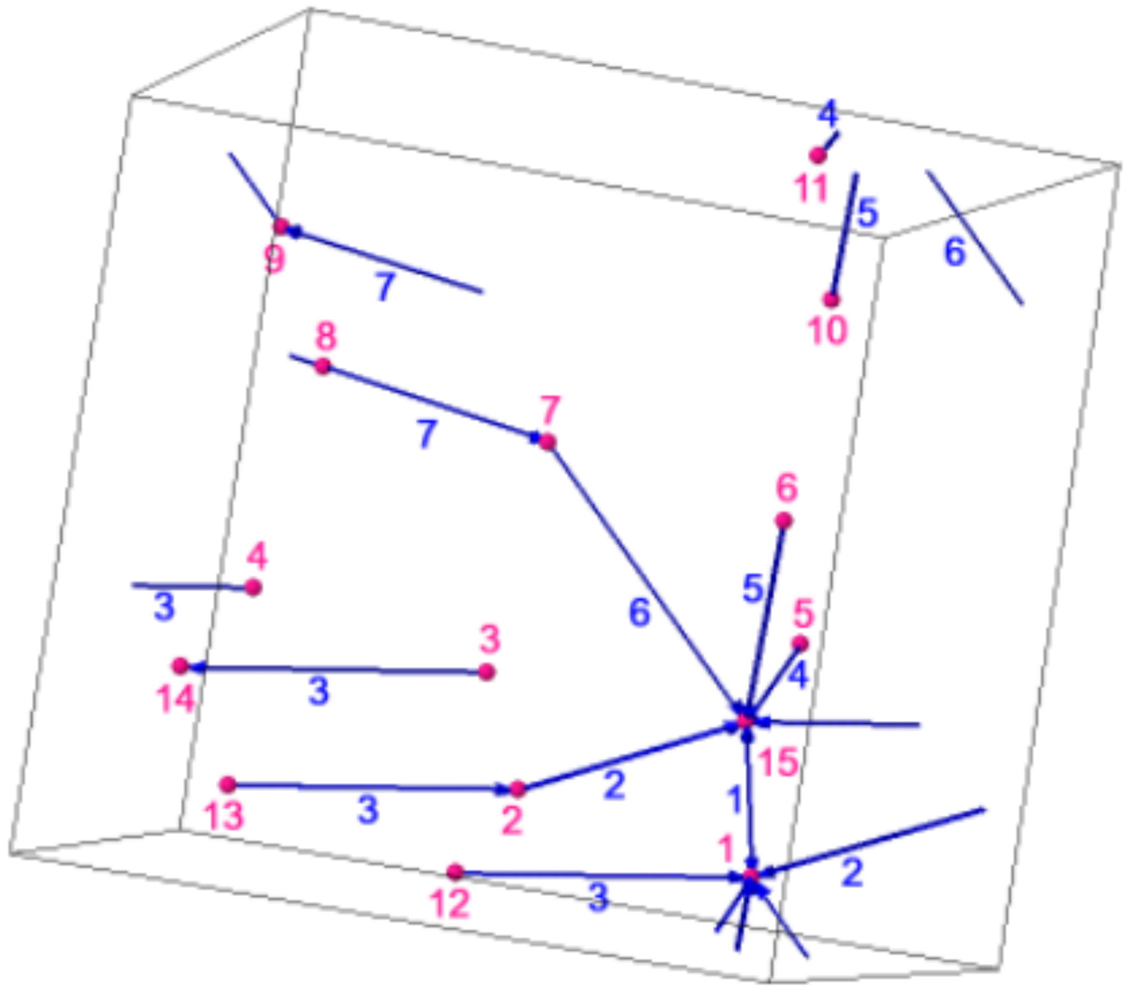


$\vec{\alpha} = (0.38, 0.132)$, $N = 9$



$\vec{\alpha} = (0.105, 0.275)$, $N = 12$

Example with 7 distances in dimension 3



$$\vec{\alpha} = \left(\frac{46}{125}, \frac{107}{500}, \frac{43}{500}\right), N = 15$$

A five distance theorem

Theorem E. (Haynes & JM, IMRN 2021)
For every $\vec{\alpha} \in \mathbb{R}^d$ and $N \in \mathbb{N}$ we have that

$$g_N \leq \begin{cases} 3 & (d=1) \\ 5 & (d=2) \\ \sigma_d + 1 & (d \geq 3) \end{cases}$$

where σ_d is the kissing number for $\mathbb{R}^d$.

3	5	13	25	46	79	135	241	365	555

- Holds also if $\mathbb{Z}^d$ is replaced by any lattice of full rank in $\mathbb{R}^d$
- Holds also if standard Euclidean metric on $\mathbb{T}^d$ is replaced by any flat Riemannian metric
- Biringer and Schmidt (2008) showed $g_N \leq 3^d + 1$ (in fact for general isometric anctions on Riemannian manifolds with sectional curvature ≥ 0)

4	10	28	82	244	730	2188	6562	19684	59050

- If metric is given by max-norm, then $g_N \leq 2^d + 1$ (Chevallier 1996 $d = 2$, Haynes & Ramirez 2020)

3	5	9	17	33	65	129	257	513	1025

Lower bounds

We say $N_1 < N_2 < N_3 < \ldots$ of integers is sub-exponential if $\lim_{i\to\infty} \frac{N_{i+1}}{N_i} = 1$.

Theorem F. (Haynes & JM, IMRN 2021)
There is a $P \subset \mathbb{R}^d$ of full Lebesgue measure, such that for every $\vec{\alpha} \in P$, $\vec{\alpha}_0 \in \mathbb{R}^d$, and for every sub-exponential sequence $(N_i)_i$, we have

$$\limsup_{i\to\infty} g_{N_i}(\vec{\alpha}) \geq \sup_{N\in\mathbb{N}} g_N(\vec{\alpha}_0).$$

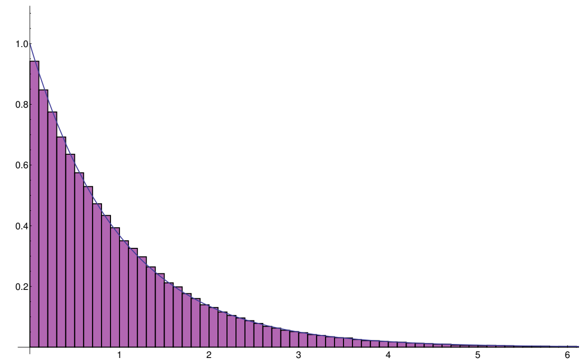
- **Corollary:** For $\vec{\alpha} \in P$ we have $\limsup_{i\to\infty} g_{N_i}(\vec{\alpha}) \begin{cases} = 5 & \text{if } d = 2 \\ \geq 9 & \text{if } d = 3^* \end{cases}$

The starting point of the above theorems is our "lattice proof" of the three gap theorem. Theorem E then requires a detailed geometric analysis on lattice configurations; Theorem F uses in addition the density of typical orbits of a certain diagonal one-parameter flow on the space of lattices.

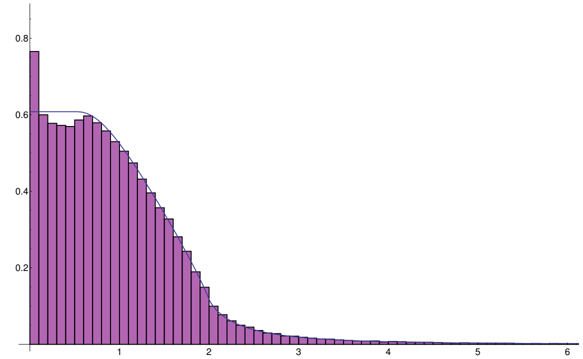
*Carl Dettmann found a numerical example with 9 distinct distances

Fractional parts of small powers

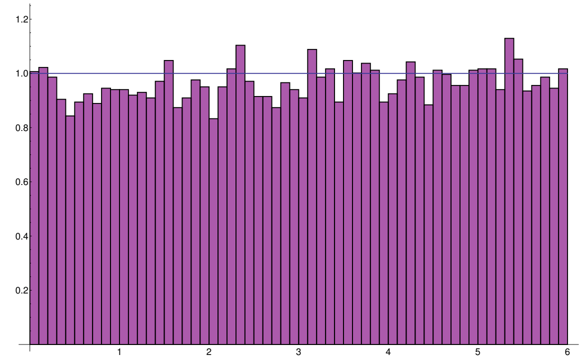
- For fixed $0 < \beta < 1$, $\beta \neq \frac{1}{2}$, the gap distribution of $n^\beta \bmod 1$ looks Poisson numerically—-NO PROOFS![*]
  The example on the right is for $\beta = \frac{1}{3}$



- For $\beta = \frac{1}{2}$, Elkies & McMullen (Duke Math J 2004) have shown that the gap distribution exists, and derived an explicit formula which is clearly different from the exponential.



- At the same time, the two-point function converges to the Poisson answer (JM, El Baz & Vinogradov, Proc AMS 2015). The proof requires upper bounds for the equidistribution of certain unipotent flows with respect to unbounded test functions.



[*]See recent proof for two-point statistics for $\beta \leq 1/3$: C. Lutsko, N. Technau & A. Sourmelidis, Pair correlation of the fractional parts of αn^θ, arXiv:2106.09800 (2021)

Fractional parts of $\sqrt{n}$

N. Elkies & C. McMullen, Duke Math J 2004

- We aim to show that the random set (here s is a random variable uniformly distributed in $[0, 1]$)

$$P_{N,s} = \{N(\sqrt{n} + m - s)) \mid n = 1, \ldots, N,\ m \in \mathbb{Z}\}$$

converges in distribution to a limit that is described by a random affine lattice. (The gap distribution will then follow as a corollary.)

- "Lift" this to the following point set in $\mathbb{R}^2$:

$$Q_{N,s} = \left\{ \left(\frac{n^{1/2}}{N^{1/2}}, N\left(n^{1/2} + m - s\right) \right) \,\middle|\, (m,n) \in \mathbb{Z}^2,\ n > 0 \right\}$$

and note that $P_{N,s} = \pi_2\left[Q_{N,s} \cap \left((0,1] \times \mathbb{R}\right)\right]$ (cut and project!).

- Here is another point set in $\mathbb{R}^2$:

$$\widetilde{Q}_{N,s} = \left\{ \left(\frac{m+s}{N^{1/2}}, -\frac{N^{1/2}(n + 2ms + s^2)}{2N^{-1/2}(m+s)} \right) \,\middle|\, (m,n) \in \mathbb{Z}^2 \right\}$$

- $Q_{N,s}$ and $\widetilde{Q}_{N,s}$ are close (in the right half plane) ...

- Fix any compact set $\mathcal{A} \subset \mathbb{R}_{>0} \times \mathbb{R}$. Then for any element in $Q_{N,s} \cap \mathcal{A}$ we have $n^{1/2} = -m + s + O_{\mathcal{A}}(N^{-1})$, so

$$\left(\frac{n^{1/2}}{N^{1/2}}, N\left(n^{1/2} + m - s\right)\right)$$
$$= \left(\frac{n^{1/2}}{N^{1/2}}, \frac{N\left(n - (-m+s)^2\right)}{n^{1/2} - m + s}\right)$$
$$= \left(\frac{-m+s}{N^{1/2}} + O_{\mathcal{A}}(N^{-3/2}), \frac{N^{1/2}\left(n - (-m+s)^2\right)}{2N^{-1/2}(-m+s) + O_{\mathcal{A}}(N^{-3/2})}\right)$$

- Now shift n by m^2 (this 1:1 on $\mathbb{Z}$) and then replace (m,n) by $-(m,n)$. This shows that each element in $Q_{N,t} \cap \mathcal{A}$ is $O(N^{-3/2})$-close to a unique point in

$$\widetilde{Q}_{N,t} = \left\{\left(\frac{m+s}{N^{1/2}}, -\frac{N^{1/2}(n+2ms+s^2)}{2N^{-1/2}(m+s)}\right) \,\middle|\, (m,n) \in \mathbb{Z}^2\right\}.$$

The key observation

- It is now an exercise to show that

$$\widetilde{Q}_{N,s} = \left\{ \left(y_1, -\frac{y_2}{2y_1} \right) \,\middle|\, (y_1, y_2) \in \mathbb{Z}^2 u(s) a(N^{-1/2}) \right\}$$

  where

$$u(s) = \left(\begin{pmatrix} 1 & 2s \\ 0 & 1 \end{pmatrix}, (s, s^2) \right), \qquad a(r) = \left(\begin{pmatrix} r & 0 \\ 0 & r^{-1} \end{pmatrix}, 0 \right) \in \mathsf{ASL}(2, \mathbb{R}).$$

  Note that $u(s)$ generates a one-parameter subgroup of $\mathsf{ASL}(2, \mathbb{R})$

- Recall $\mathsf{ASL}(2, \mathbb{R}) = \mathsf{SL}(2, \mathbb{R}) \ltimes \mathbb{R}^2$ with multiplication law

$$(M, z)(M', z') = (MM', zM' + z')$$

Limit theorems

- Set $G = \mathrm{ASL}(2,\mathbb{R})$, $\Gamma = \mathrm{ASL}(2,\mathbb{Z})$, $X = \Gamma\backslash G$. It follows from Ratner's measure classification theorem* that for $f : X \to \mathbb{R}$ bounded continuous, λ absolutely continuous Borel probability measure on $[0,1]$, and $r \to 0$,

$$\int_0^1 f(\Gamma u(s)a(r))\lambda(ds) \to \int_X f(g)d\mu(g)$$

- Following our previous strategy, this implies convergence

$$\mathbb{Z}^2 u(s)a(r) \xrightarrow{\mathrm{d}} \mathbb{Z}^2 g$$

to a (Haar-) random affine lattice

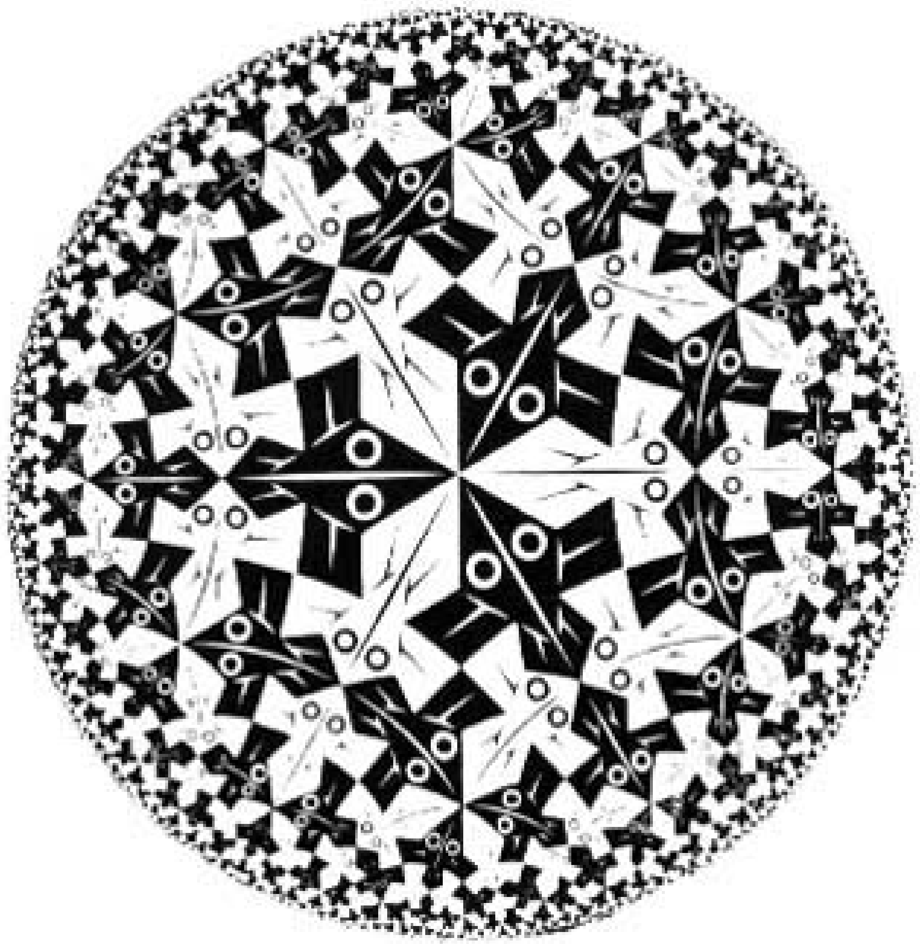
- This in turn implies in view of the previous calculation, via cut and project,

$$P_{N,s} = \{N(\sqrt{n} + m - s)) \mid n = 1,\ldots,N,\ m \in \mathbb{Z}\}$$
$$\xrightarrow{\mathrm{d}} \left\{ -\frac{y_2}{2y_1} \,\middle|\, (y_1,y_2) \in \mathbb{Z}^2 g,\ y_1 \in (0,1] \right\}$$

- From this the convergence of the gap distribution and its formula follow.

*For an effective proof see T. Browning, I. Vonogradov, J. LMS 2016, building on the crucial work by A. Strömbergsson, Duke Math. J. 2015

How about random lattices in hyperbolic geometry?



Escher's Circle Limit I

Random hyperbolic lattices

- $G = \mathsf{SL}(2,\mathbb{R})$ acts by Möbius transformations on complex upper half plane

$$\mathbb{H} \to \mathbb{H}, \qquad z \mapsto \frac{az+b}{cz+d}, \qquad \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G$$

- $\Gamma < G$ Fuchsian subgroup of finite co-volume

- For $w \in \mathbb{H}$ consider the hyperbolic lattice Γw in $\mathbb{H}$

- Deform Γw by $g \in G$ to obtain $g\Gamma w$

- The space of such lattices is parametrized by G/Γ, which carries a (unique) G-invariant probability measure μ

- We can define the μ-random hyperbolic lattice $g\Gamma w$

Directions in hyperbolic lattices

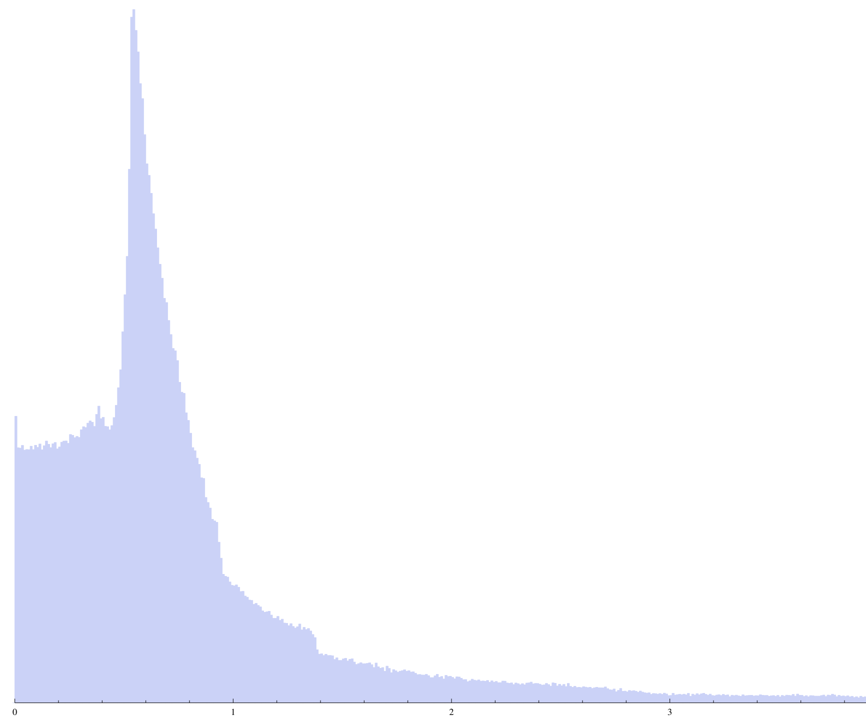
- Previous work on two-point statistics by F. Boca, V. Paşol, A. Popa, A. Zaharescu (2014), D. Kelmer & A. Kontorovich (2015), M. Risager & A. Södergren (2017)

- As for Euclidean lattices and quasicrystals, can now study distribution of angles of hyperbolic lattice points Γw, as seen from an observer at the origin $\mathrm{i} \in \mathbb{H}$

- The convergence of the gap distribution follows from the convergence of the point processes

$$\begin{pmatrix} \epsilon^{-1} & 0 \\ 0 & \epsilon \end{pmatrix} \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} \Gamma w \xrightarrow{\mathrm{d}} g\Gamma w$$

as $\epsilon \to 0$, with θ a uniform random variable in $[0, 2\pi]$, g is μ-random.



Gap distribution

JM and I. Vinogradov, Directions in hyperbolic lattices, Crelle 2018

Random hyperbolic lattices and roots of quadratic congruences

- Consider the roots μ of the quadratic congruence

$$\mu^2 \equiv D \pmod{m}$$

with $m = 1, 2, 3, \ldots$ and $D > 0$ square-free (all will work also for $D < 0$; it's easier)

- Define sequence $\xi_1, \xi_2, \ldots \in \mathbb{T} = \mathbb{R}/\mathbb{Z}$ by normalised roots $\frac{\mu}{m}$, ordered by increasing denominator m (choose arbitrary order for terms with same m)

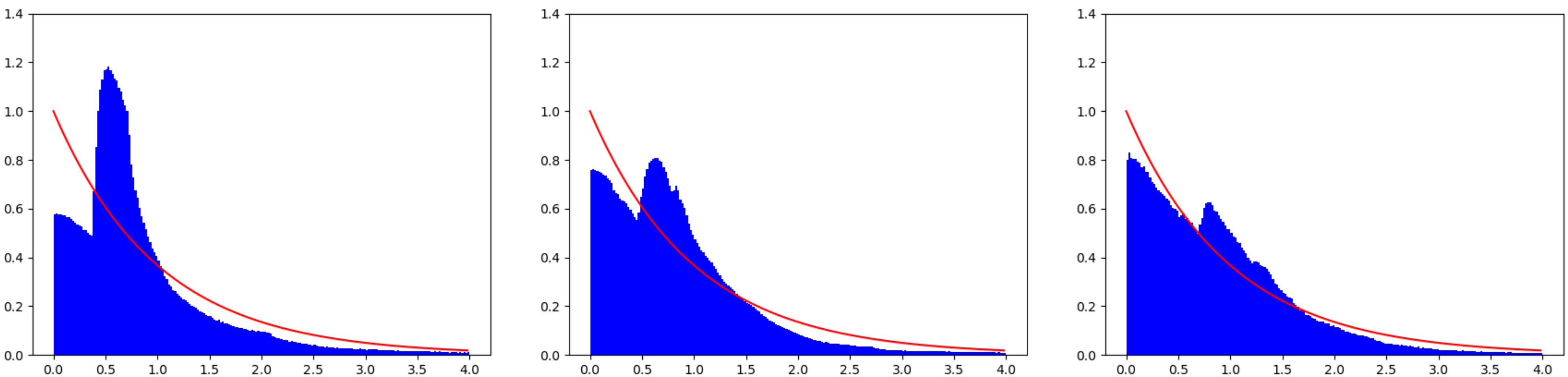
- C. Hooley (1963): We have uniform distribution mod 1

$$\lim_{N\to\infty} \frac{1}{N} \#\left\{ j \leq N : \xi_j \in [a, b) + \mathbb{Z} \right\} = b - a$$

- Extension to higher-order polynomial congruences (C. Hooley 1964); use of modular forms, Poincaré series (V.A. Bykovskii 1984; see also A. Good 1983); u.d. still holds for m restricted to primes (W. Duke, J. Friedlander, H. Iwaniec 1995); joint distribution (S. Zahavi 2020); fits in more general CRT framework (E. Kowalski and K. Soundararajan 2020).

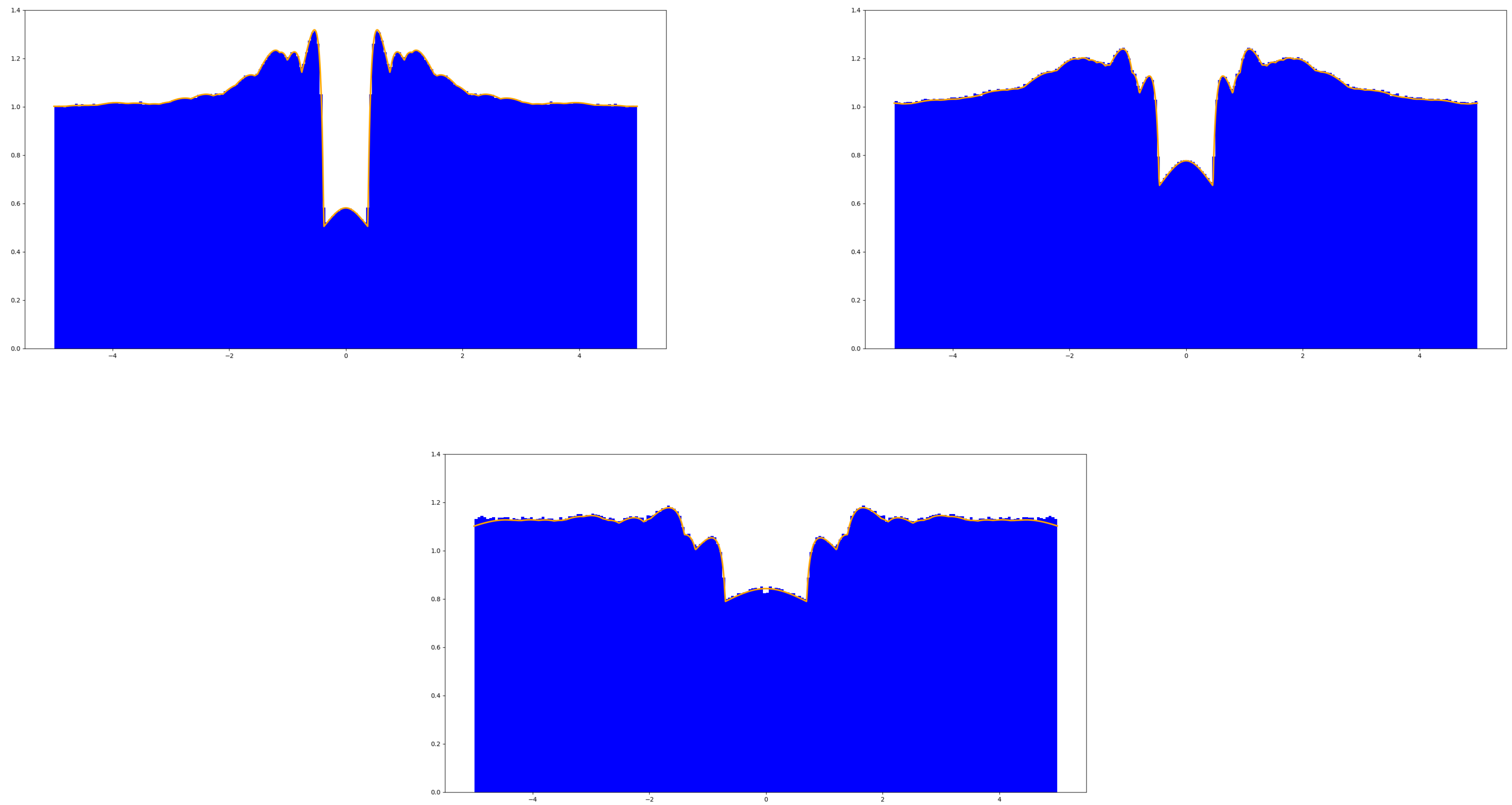
Gaps between roots

Theorem G. (JM & M. Welsh, Duke Math. J., in press)
Let $D > 0$ square-free, $D \not\equiv 1 \bmod 4$. Then the distribution of gaps between the elements of the finite sequence $(\xi_j)_{j=1}^N$ converges weakly to limit with continuous distribution function.



$$D = 2, 3, 10 \qquad N = 10^6$$

Two-point statistics



$$D = 2, 3, 10 \qquad N = 10^6$$

Here we consider distances between all (rather than just consecutive) elements. The red curve is our theoretic prediction.

Key insight: the geometry of roots

Theorem H. (JM & M. Welsh, Duke Math. J., in press)
For D as above, there exists a finite set of geodesics $\{\boldsymbol{c}_1, \dots, \boldsymbol{c}_h\}$ such that:

(i) For any $m > 0$ and μ satisfying $\mu^2 \equiv D \pmod{m}$, there is a unique geodesic of the form $\gamma \boldsymbol{c}_l \subset \mathbb{H}$ with $\gamma \in \mathrm{SL}(2, \mathbb{Z})$ and its top at the point

$$\frac{\mu}{m} + \mathrm{i}\frac{\sqrt{D}}{m}$$

(ii) Conversely, given any geodesic of the above form, there exist unique $m > 0$ and $\mu \pmod{m}$ satisfying $\mu^2 \equiv D \pmod{m}$.

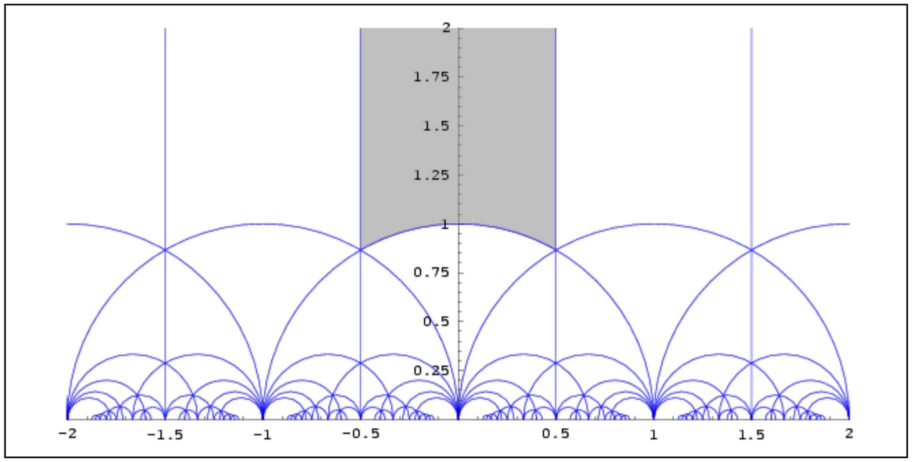
- The geodesics $\{\boldsymbol{c}_1, \dots, \boldsymbol{c}_h\}$ project to closed geodesics of equal length in $\mathrm{SL}(2, \mathbb{Z})\backslash\mathbb{H}$
- Extends to setting with additional congruence conditions $m \equiv 0 \pmod{n}$, and $\mu \equiv \nu \pmod{n}$, need to replace $\mathrm{SL}(2, \mathbb{Z})$ by $\Gamma_0(n)$
- See M. Welsh (Algebra & Number Th. 2022) for parametrization of roots of higher-degree polynomial congruences

Geodesic line processes

- $\boldsymbol{c}$ geodesic in $\mathbb{H}$ that projects to closed geodesic in $\Gamma\backslash\mathbb{H}$

- Corresponding stabiliser subgroup $\Gamma_{\boldsymbol{c}}$ $= \{g \in \mathrm{SL}(2,\mathbb{R}) : g\boldsymbol{c} = \boldsymbol{c}\} < \Gamma$

- Consider orbit of geodesic $\Gamma\boldsymbol{c} = \{\gamma\boldsymbol{c} : \gamma \in \Gamma/\Gamma_{\boldsymbol{c}}\}$



- Deform by $g \in G$ to obtain $g\Gamma\boldsymbol{c} = \{g\gamma\boldsymbol{c} : \gamma \in \Gamma/\Gamma_{\boldsymbol{c}}\}$

- The space of such unions of geodesics is again parametrized by G/Γ

- We can define the μ-random line process $g\Gamma\boldsymbol{c}$, with g distributed according to the (unique) G-invariant probability measure μ

- **Use convergence** $\begin{pmatrix} \epsilon^{-1} & 0 \\ 0 & \epsilon \end{pmatrix} \begin{pmatrix} \cos\phi & -\sin\phi \\ \sin\phi & \cos\phi \end{pmatrix} \Gamma\boldsymbol{c} \xrightarrow{\mathrm{d}} g\Gamma\boldsymbol{c}$ **to prove Theorem A**

Outline

Lecture 1 What are random lattices? Basic features and examples

Lecture 2 Random lattices in number theory and geometry

Lecture 3 Random lattices in statistical mechanics – the Lorentz gas (tomorrow)