

Equidistribution in Number Theory

MA841 BU Fall 2018

Salim Ali Altuğ

September 19, 2018

1 Equidistribution in Number Theory

Lecture 1 6/9/2018

These are notes for Ali Altuğ's course MA841 at BU Fall 2018.

The course webpage is http://math.bu.edu/people/saaltug/2018_3/2018_3_sem.html.

Course overview: Upon Akshay Venkatesh winning the fields medal I decided to dedicate this term to various aspects of equidistribution results in number theory and their relations to L-functions. I am aiming to cover basic results like Linnik's and Duke's theorems, as well as certain aspects of subconvexity. As we move along we may briefly touch several other aspects like quantum unique ergodicity (QUE) or equidistribution in other settings (e.g. over function fields). There is an abundance of material on this topic. We will not follow a single book or an article (although the first book and the survey articles following that will be the main reference), however here are a bunch of helpful papers/books. I will update these references as we move along.

1.1 Introduction

I wasn't going to do this at all, but then Akshay won the Fields medal.

—Ali Altuğ

Some topics we will try and cover:

1. Linnik's and Duke's theorem 1970-1990
2. lattice points and hyperbolic geometry
3. modular forms
4. spectral theory
5. modular forms of half integral weight.
6. harmonic analysis
7. Kuznetsov formula
8. Other topics!

1.2 Linnik and Duke

Akshay's first breakthrough, according to Sarnak, was subconvexity. He became interested in ergodic theory, because they could prove hard theorems, equidistribution is a powerful tool in number theory.

Our main goal will be to talk about: Some problems stated (and proved) by Linnik. In the book, *Ergodic properties of algebraic fields*, 1968. He considered lattice points on a sphere of radius n , these are points (say in \mathbf{R}^3) whose coordinates are integral of a fixed distance from the origin. Analogous to the circle problem. If n is fixed there is nothing to distribute, but if we vary n and project down we can ask do they accumulate miss any patches, generally how do they distribute. Of course this can be generalised.

Setup Sphere S^2 .

Lattice points $\alpha = (x_1, x_2, x_3) \in \mathbf{Z}^3$.

$$|\alpha|^2 = x_1^2 + x_2^2 + x_3^2$$

this is where the number theory comes, we are looking at representability of numbers n by this ternary quadratic form.

Various methods exist for studying this for varying n , quadratic reciprocity for $n = 2$, circle method/Vinogradov for $n = 4$. $n = 3$ is the cut off, here half integral weight modular forms are relevant.

Set

$$\Omega_N = \left\{ x = \frac{\alpha}{|\alpha|} : \alpha \in \mathbf{Z}^2, |\alpha|^2 = N \right\} \subseteq S^2.$$

Question 1.1 Are Ω_N "equidistributed" as $N \rightarrow \infty$? □

There is an immediate obstruction to N being a sum of 3 squares, e.g. $N = 7$ implies $\Omega_7 = \emptyset$.

Recall: (Gauss/Legendre)

$$N = x_1^2 + x_2^2 + x_3^2, x_i \in \mathbf{Z} \iff N \neq 4^a(8b+7),$$

so we avoid these sets and ask the same question.

Theorem 1.2 Linnik. Let $f \in C^\infty(S^2)$, then as $N \rightarrow \infty$, N squarefree $N \not\equiv 7 \pmod{8}$, $\left(\frac{N}{p}\right) = 1$ for some fixed odd prime p

$$\frac{1}{\#\Omega_N} \sum_{x \in \Omega_N} f(x) \rightarrow \int_{S^2} f \, d\sigma$$

where $d\sigma$ is the Lebesgue measure on S^2 .

This is saying that the points are equidistributed with respect to the Lebesgue measure.

The last condition is a defect of the method, known as a Linnik condition.

Remark 1.3 Linnik's proof is ergodic theoretic.

After this came Duke in 1988, in the mean time, Weil conjectures were proved, Iwaniec gave bounds for Kloosterman sums. Duke was a graduate student of Sarnak at Courant. He gave a more direct proof of [Theorem 1.2](#) which does not have the $\left(\frac{N}{p}\right) = 1$ condition. His proof is based on the theory of (half integral weight) modular forms, and a good bound Iwaniec on certain exponential sums.

Why do exponential sums enter the picture? We are trying to prove that we have a sum converging to an integral. Generally we work with a basis of

functions first, we could try using fourier analysis, using harmonics as our basis, this is when exponential sums appear. That requires us to work out harmonics on the sphere (spherical harmonics) which leads to representation theory, which as the sphere is compact involves Weyl representations etc.

Duke also proved “the same” theorem over modular surfaces. Instead of looking at expanding spheres we study expanding hyperboloids.

Setup Space

$$\begin{aligned} & \pm\Gamma\backslash\mathbf{H} \\ \mathbf{H} &= \{x + iy \in \mathbb{C} : y > 0\} \\ \Gamma &= \mathrm{SL}_2(\mathbb{Z}) \\ \mathcal{F} &= \left\{ z \in \mathbf{H} : -\frac{1}{2} \leq \Re(z) \leq 0, |z| \geq 1 \text{ or } \frac{1}{2} > \Re(z) > 0, |z| > 1 \right\} \end{aligned}$$

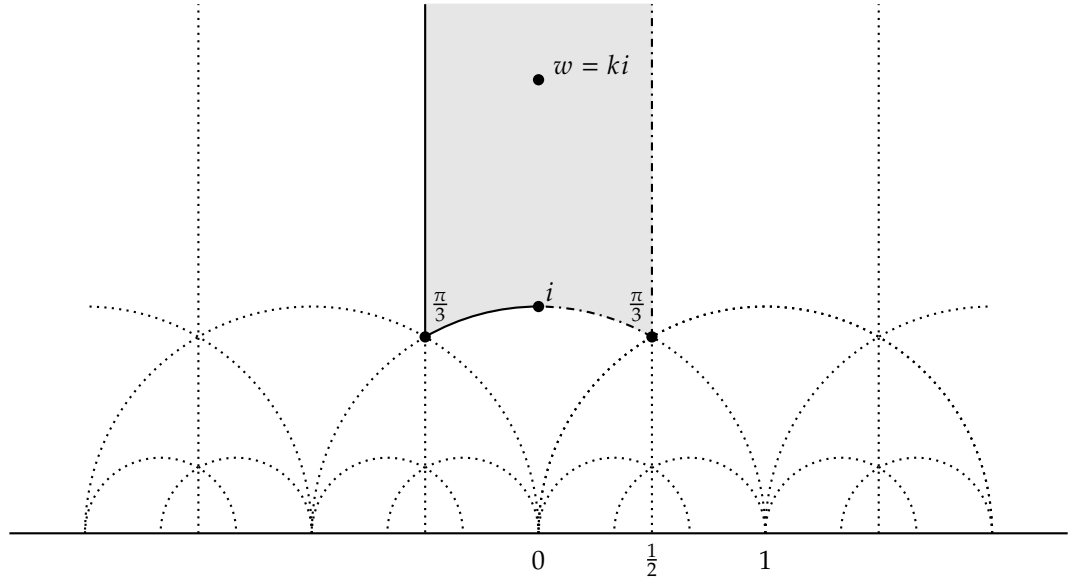


Figure 1.4: \mathcal{F}

Ω_N 's are now replaced with CM points.

Digression (CM points) Q a binary quadratic form

$$Q(x, y) = ax^2 + bxy + cy^2$$

of discriminant $d = b^2 - 4ac < 0, a, b, c \in \mathbb{Z}$.

Theorem 1.5 Gauss. *There are only finitely many equivalence classes of such forms for fixed d .*

The number of such is given by the Hurwitz class number.

Given Q we associate a CM point

$$z_Q = \frac{-b + \sqrt{d}}{2a} \in \mathbf{H}.$$

The action of Γ on Q is the same as the action of Γ on z_Q .

$$z_{\gamma Q} = \gamma z_Q.$$

Let

$$\Lambda_d = \{z_Q \in \mathcal{F} : \text{disc}(Q) = d\}.$$

We need to sum properly to take automorphisms into account.

Definition 1.6

$$\sum_{z_Q \in \Lambda_d}^*$$

is the sum weighted by $\frac{1}{2}$ if $Q = a(x^2 + y^2)$ ($d = -4$), $\frac{1}{3}$ if $Q = a(x^2 + xy + y^2)$ ($d = -3$). \diamond

If we want to be fancy we can say the word stack here.

Remark 1.7

$$\sum_{z_Q \in \Lambda_d}^* 1 = H(d)$$

where $H(d)$ is the Hurwitz class number.

Remark 1.8 If d is fundamental, i.e. a discriminant of some $\mathbf{Q}(\sqrt{d})$ then $H(d) = h(d)$ the regular class number.

For the measure on \mathcal{F} we take

$$d\mu = \frac{3}{\pi} \frac{dx dy}{y^2}.$$

Theorem 1.9 Duke. Let $f \in C^\infty(\mathbf{H})$, that is Γ invariant and bounded on \mathcal{F} , then as $d \rightarrow \infty$ over fundamental discriminants

$$\frac{1}{\#\Lambda_d} \sum_{z \in \Lambda_d}^* f(z) \rightarrow \iint_{\mathcal{F}} f d\mu.$$

Equidistribution implies density, but is so much more, for example we cannot have dense points but which happen to cluster towards some line for example.

1.3 Basics

Lecture 2 11/9/2018

Question: Let $\alpha \in \mathbf{R}$ and consider $\{\alpha n\}$ where $\{x\} = x \pmod{1}$ so $\{\frac{3}{2}\} = \frac{1}{2}$. How are these distributed?

Example 1.10 If $\alpha = \frac{2}{7}$ then we have $\{\{\alpha n\} : n \in \mathbf{N}\} = \{\frac{i}{7} : i \in \{0, \dots, 6\}\}$ and in fact it hits each evenly. \square

Example 1.11 If $\alpha = \sqrt{2}$ so $\{\alpha\} \approx 0.4142? \dots$ $\{\alpha 2\} \approx 0.8284? \dots$ $\{\alpha 3\} \approx 0.24264 \dots$ $\{\alpha 4\} \approx 0.656854 \dots$ These spread out densely, but there is a difference between density and equidistribution. In this example, equidistribution says that the proportion of time the sequence spends in each interval (a, b) is $b - a$. \square

So questions are: is $\{n\alpha\}$ dense?

Is $\{n\alpha\}$ **uniformly distributed** (equidistributed with respect to the standard measure)?

The answer to both questions is yes.

Theorem 1.12 Kronecker. Let $\alpha \in \mathbf{R} \setminus \mathbf{Q}$ then $\{n\alpha\}$ is dense in $[0, 1)$.

Digression (Diophantine approximation) This is a very tough area of number theory, not so many definitive results here.

Theorem 1.13 Dirichlet. Let $\alpha \in \mathbf{R}, N \in \mathbf{Z}_{>0}$ then there exists p, q with $q > 0$.

$$|q\alpha - p| < \frac{1}{N}.$$

Proof. (Pidgeonhole) divide $[0, 1)$ into even N subintervals of width $\frac{1}{N}$, consider

$$\alpha_0 = 0, \alpha_1 = \{\alpha 1\}, \alpha_2 = \{\alpha 2\}, \dots \in [0, 1)$$

as soon as we get to α_N we must have two in one subinterval say $|\alpha_{n_1} - \alpha_{n_2}| < \frac{1}{N}$. So there exists p_{n_1}, p_{n_2} such that

$$|n_1\alpha - k_{n_1} - (n_2\alpha - k_{n_2})| < \frac{1}{N}$$

$$|(n_1 - n_2)\alpha - (k_{n_1} - k_{n_2})| < \frac{1}{N}. \quad \blacksquare$$

Corollary 1.14 Let $\alpha \in \mathbf{R} \setminus \mathbf{Q}$ then there exists infinitely many coprime p, q with $q > 0$ satisfying

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}.$$

Proof. Exercise. \blacksquare

This is very strong, Roth's theorem tells us that even $q^{2+\epsilon}$ here is enough to force finiteness.

Note 1.15 $\alpha \notin \mathbf{Q}$ is necessary! Otherwise

$$\left| \frac{p_0}{q_0} - \frac{p}{q} \right| = \left| \frac{p_0q - pq_0}{qq_0} \right| \geq \frac{|p_0q - pq_0|}{\max\{q^2, q_0^2\}}$$

so choose $q > q_0$ implies $\frac{p_0}{q_0} = \frac{p}{q}$.

One can do better:

Theorem 1.16 Hurwitz. Let $\alpha \in \mathbf{R} \setminus \mathbf{Q}$

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{\sqrt{5}q^2}$$

then there exists infinitely many coprime p, q with $q > 0$ satisfying.

Note 1.17 $\sqrt{5}$ is the best possible without further restriction on α .

Example 1.18 If $\alpha = \frac{1-\sqrt{5}}{2}$ then

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{Aq^2}$$

has only finitely many solutions for $A > \sqrt{5}$. \square

What if we allow further restriction?

Theorem 1.19 Liouville. Let $\alpha \in \mathbf{R}$ algebraic of degree $n > 1$. Then there exists $A > 0$ such that for all p, q with $q > 0$

$$\left| \alpha - \frac{p}{q} \right| > \frac{A}{q^n}.$$

Proof. Let $f \in \mathbb{Z}[x]$ be the minimal polynomial of α . Gauss's lemma implies that f is irreducible over \mathbb{Q} so

$$q^n f\left(\frac{p}{q}\right) \in \mathbb{Z} \setminus \{0\} \forall \frac{p}{q} \in \mathbb{Q}.$$

The mean value theorem says that there exists $x_0 \in [\alpha, p/q]$ s.t.

$$\frac{f(p/q) - f(\alpha)}{p/q - \alpha} = f'(x_0)$$

so

$$\frac{q^n f(p/q)}{q^n f'(x_0)} = |p/q - \alpha|,$$

notice how n appears here. ■

This theme of using some calculus is repeated across diophantine analysis.

Remark 1.20

- Thue: can replace n with $(\deg(\alpha) + 2)/2$ (This already has implications to integral solutions of degree ≥ 3 polynomials $f \in \mathbb{Z}[x]$, e.g. elliptic curves with bounded integral discriminant)
- Roth (~ 1958): for all $\epsilon > 0$, there are only finitely many p/q satisfying

$$|\alpha - \frac{p}{q}| < \frac{1}{q^{2+\epsilon}}.$$

Back to equidistribution $a_n = \{n\alpha\}, \{a_n\}_{n=1}^\infty$.

Theorem 1.21 Kronecker. a_n is dense in $[0, 1)$ if $\alpha \notin \mathbb{Q}$.

Proof. Will show for any $x \in [0, 1)$ there exists

$$\{a_{n_j}\}_{j=1}^\infty \text{ s.t. } a_{n_j} \rightarrow x.$$

Notation $\|x\|$ means the distance to the nearest integer. Dirichlet implies that infinitely many p/q have $|\alpha - p/q| < 1/q^2$. Given $\epsilon > 0$ let q be such that

$$|\alpha - \frac{p}{q}| < \frac{1}{q^2} \implies |q\alpha - p| < \frac{1}{q}$$

$$\frac{1}{q} < \epsilon$$

Choose j such that $j(\alpha q - p)$ is within $1/q$ of x (why?). So

$$\|j(\alpha q - p) - x\| < \frac{1}{q} < \epsilon.$$

(Fill in the gaps here). ■

Now let's define what it means to be **uniformly distributed**.

Definition 1.22 Uniformly distributed sequence. a_1, a_2, \dots is called **uniformly distributed** if for all $(b, c) \subseteq [0, 1)$

$$\#\{n \leq N : \{a_n\} \in (b, c)\} \sim N(c - b)$$

or

$$\lim_{N \rightarrow \infty} \frac{\#\{n \leq N : \{a_n\} \in (b, c)\}}{N} = c - b.$$

◇

Uniformly distributed or not?

When $\alpha \in \mathbf{R} \setminus \mathbf{Q}$: $\{n\alpha\}$, $\{n^2\alpha\}$, $\{(3n^2 + 2n + 1)\alpha\}$, $\{(\sqrt{5}n^3 + 2n - (\zeta_{10} + \bar{\zeta}_{10}))\alpha\}$ all are.

$\{n!e\}$, $\{\log(n)\}$ and $\{\log(p_n)\}$ are not.

Lecture 3 13/9/2018

Example 1.23 Several.

1. $\alpha \in \mathbf{R} \setminus \mathbf{Q}$, $a_n = \{n\alpha\}$. Yes
2. $\alpha \in \mathbf{R} \setminus \mathbf{Q}$, $a_n = \{n^2\alpha\}$. Yes
3. $a_n = \{\log(n)\}$. No
4. $a_n = \{n!e\}$. No (not dense).
5. $\{\log(p_n)\}$. No.
6. $a_n = \{\sqrt{n}\}$. Yes.
7. $a_n = \{e^n\}$. ?
8. $a_n = \{\log n!\}$. Yes ?
9. $a_n = \{\log \log n!\}$. No

To begin let's show $a_n = \{n!e\}$ is not equidistributed as it has only one limit point 0.

$$e = \sum_{n=1}^{\infty} \frac{1}{n!}$$

so $n!e \in \mathbf{Z} + \frac{1}{n+1} + \frac{(n+1)(n+2)}{+} \dots \leq \frac{e}{n+1} \rightarrow 0$, as $n \rightarrow \infty$. So its not dense, hence certainly not equidistributed. □

Theorem 1.24 The sequence $a_n = \{n\alpha\}$ is equidistributed.

Proof. Let $\epsilon > 0$, choose $M > 0$ such that $\frac{1}{M} < \epsilon$, furthermore choose a $\delta < \frac{1}{M}$. Dirichlet implies there exists $m \in \mathbf{Z}$ s.t. $\|m\alpha\| = \delta$.

$$0 < \delta < \frac{1}{M} < \epsilon$$

recall $\|x\|$ is the distance to the nearest integer. Consider the set $S_i = \{\{n\alpha\} : n < N, n \equiv i \pmod{m}\}$ then

$$S = \{\{n\alpha\} : n < N\} = \bigsqcup_{i=1}^m S_i$$

moreover,

$$S_i = \{\{km\alpha + i\alpha\} : 0 \leq k \leq N_i\}$$

where

$$N_i = \frac{N}{m} + O(1)$$

(why is the $O(1)$ here?). We can rewrite these S_i as follows:

$$S_i = \{\delta k + \gamma_i \pmod{1} : 0 \leq k \leq N_i\}$$

where

$$\begin{cases} i\alpha \pmod{1} & \text{if } \delta = \{m\alpha\} \\ i\alpha - \delta(N_i + 1) \pmod{1} & \text{if } \delta = 1 - \{m\alpha\} \end{cases}$$

replace k by $N_i + 1 - k$.

Now $0 \leq \gamma < 1$ and let

$$K_i = \lfloor \delta N_i + \gamma_i \rfloor$$

$$\#\{k < N_i : \{\delta k + \gamma_i\} \in [b, c]\} = \sum_{j=0}^{K_i} \#\{k \leq N_i : \delta k + \gamma \in [j + b, j + c]\}$$

$$= (K_i + O(1)) \left(\frac{c - b}{\delta} + O(1) \right)$$

$$N_i(c - b) + O\left(\frac{c - b}{\delta} + \delta N_i + 1\right)$$

so

$$S = \bigsqcup_{i=1}^m S_i$$

$$\#S = N(c - b) + O\left(\frac{M}{\delta} + \delta N\right)$$

(check!). Finally choose $N > \frac{M}{\delta^2}$. So that

$$\frac{M}{\delta} + \delta N < \epsilon N.$$

Which implies

$$\#\{n < N : \{n\alpha\} \in [b, c]\} = \#S = N(c - b) + \epsilon N. \quad \blacksquare$$

We followed our nose essentially, but we needed to put ourselves in a favourable position so that we can get a good handle on the error.

Example 1.25 10. Consider the sequence

$$b_{m,i} = \frac{i}{m}$$

and define

$$a_{\binom{m}{2}+i} = b_{m,i}$$

so that

$$b_{m,i}$$

$$0, 1$$

$$0, \frac{1}{2}, 1$$

$$0, \frac{1}{3}, \frac{2}{3}, 1$$

$$0, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}, 1$$

$$a_m = 0, 1, 0, \frac{1}{2}, 1, 0, \frac{1}{3}, \frac{2}{3}, 1, 0, \frac{1}{4}, \frac{2}{4}, \frac{3}{4}, 1$$

this is uniformly distributed!

□

Exercise 1.26 Prove this (in a similar way to before).

Proposition 1.27

1. Any sequence has a rearrangement that is not *uniformly distributed*.
2. Any dense sequence has a rearrangement that is *uniformly distributed*.

Proof.

1. If not sense we are done already. Otherwise let $I_1 = [0, \frac{1}{2})$, $I_2 = [\frac{1}{2}, 1]$
Let $X = \{a_n \in I_1\}$, $Y = \{a_n \in I_2\}$, so both sets are infinite. Let $b_n = x_1, \dots, x_{10^{10}}, y_1, x_{10^{10}+1}, \dots, x_{20^{20}}, \dots$ so $\#\{n : b_n \in [4/5, 1]\} \sim \frac{N}{10^{10}}$.
2. If a_n is dense then, let

$$b_{n,i} = a_m \text{ s.t. } \frac{i-1}{n} < a_m < \frac{i}{n}$$

by the example above this is equidistributed.

■

What can we say about the space of *uniformly distributed* sequences? Is it closed under addition? No ($a_n = -b_n$). $\{ka_n\}$ neither ($a_n = \alpha n$, $\frac{1}{\alpha}a_n = n$). a_nb_n doesn't work either, but if b_n converges then a_nb_n is *uniformly distributed*.

1.4 Weyl's criterion (1916)

Theorem 1.28 Weyl. $\{a_n\}_{n=1}^{\infty} \in \mathbf{R}$ then TFAE:

1. $\{a_n\}_{n=1}^{\infty}$ is *uniformly distributed mod 1*.
2. $\forall f \in C([0, 1])$

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N f(\{a_n\}) = \int_0^1 f \, dx.$$

- 3.

$$\lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N e(ma_n) = \delta_m, \forall m \in \mathbf{Z}$$

where $e(x) = e^{2\pi i x}$,

$$\delta_m = \begin{cases} 0 & m \neq 0 \\ 1 & m = 0 \end{cases}.$$

Proof. 1. \implies 2..

Lecture 4 18/9/2018

1. means 2. is true for the characteristic function of $[b, c]$, hence true for step functions (because everything is linear).

Recall that any $f \in C([0, 1])$ is the uniform limit of such functions.

Exercise: Choose one that is ϵ close to f and finish the proof.

2. \implies 1.. Find $f_1, f_2 \in C([0, 1])$ such that $f_1(x) \leq \chi_{(b,c)}(x) \leq f_2(x)$ s.t.

$$\int f_1 - \chi_{(b,c)} \leq \epsilon$$

Exercise, finish this proof.

2. \implies 3.. Obvious.

3. \implies 2.. Recall Fejér's theorem that $f \in C[0, 1]$ is the uniform limit of its fourier series. Pick an $n \in \mathbf{N}$ s.t.

$$f_n(x) - \epsilon \leq f(x) \leq f_n(x) + \epsilon.$$

Exercise, finish this proof. ■

Using this we can tackle more examples, e.g.:

1. $\{\alpha p_n\}$, n -th primes, $\alpha \in \mathbf{R} \setminus \mathbf{Q}$.
2. $\{\sqrt{n}\}$
3. $\{\log(n)\}$
4. $\{\log(p_n)\}$
5. $\{\beta^n\}$, $\beta \in \mathbf{R}$.
6. $\{\alpha a_n\}$, $a_n \in \mathbf{Z}$

1.5 Some applications of Weyl's criterion

Application 1 $\{n\alpha\}$ is **uniformly distributed** iff $\alpha \in \mathbf{R} \setminus \mathbf{Q}$. Let

$$S_N(h, \alpha) = \sum_{n=0}^N e(h\alpha n)$$

then

$$S_N(h, \alpha) = \frac{e((N+1)h\alpha) - 1}{e(h\alpha) - 1}.$$

Then $e(h\alpha) - 1 \neq 0$ for all $h \in \mathbf{Z} \setminus \{0\}$ iff $\alpha \notin \mathbf{Q}$ so $S_N(h, \alpha) = O_{h,\alpha}(1)$ iff $\alpha \notin \mathbf{Q}$. So $\lim_{N \rightarrow \infty} S_N(h, \alpha) = 0$, $\forall h \neq 0 \iff \alpha \notin \mathbf{Q}$. And $S_N(0, \alpha) = N + 1$ which implies

$$\lim_{N \rightarrow \infty} \frac{1}{N} S_N(0, \alpha) = 1$$

so by Weyl's criterion $\{n\alpha\}$ is **uniformly distributed** if $\alpha \notin \mathbf{Q}$.

Digression

Theorem 1.29 Vinogradov 1937. $\{\alpha p_n\}$ is **uniformly distributed** iff $\alpha \notin \mathbf{Q}$.

He actually showed weak Goldbach conjecture, Every (sufficiently large) odd integer is a sum of 3 primes. No bound by Vinogradov, Borozdin gave a large bound, Helfgott brought it down to reality.

Application 2

$$\{\beta^n\}$$

Theorem 1.30 Koksma 1935. For almost every (Lebesgue) $\beta \in \mathbf{R}_{>1}$, $\{\beta^n\}$ is equidistributed.

Koksma was a Dutch student of Van der Corput.

Theorem 1.31 Weyl. Let $|a_n| \rightarrow \infty$ be a sequence of integers, the set of $\alpha \in \mathbf{R}$ such that αa_n is not **uniformly distributed** has Lebesgue measure 0.

Application 3

$$\{\log(n)\}$$

is not equidistributed.

Exercise 1.32 Prove this. Hint : assume it was

$$\#\{n < 1001N : \} = \#\{n < 1000N : \} + \#\{1000N \leq n \leq 1001N : \}$$

then

$$\log(n) - \log(100N + n_1) = \log(1000N) + \log(1 + n_1/1000N)$$

Application 4

$$\{\sqrt{n}\}$$

Before this, lets introduce

Definition 1.33 Discrepancy. Let $a_n \in [0, 1)$ be a sequence and $N \in \mathbf{Z}_{\geq 0}$ we define

$$D_N = \sup_{0 \leq b \leq c \leq 1} \left| \frac{\#\{n < N : a_n \in [b, c]\}}{N} - (c - b) \right|.$$

◇

Some useful lemmas:

Lemma 1.34 Let

$$D_N^* = \sup_{0 \leq c \leq 1} \left| \frac{\#\{n < N : a_n \in [0, c]\}}{N} - c \right|$$

then

$$D_N^* \rightarrow 0 \iff D_N \rightarrow 0.$$

Proof. Exercise (hint squeeze). ■

Lemma 1.35 a_n is *uniformly distributed* $\iff D_N \rightarrow 0 \iff D_N^* \rightarrow 0$.

Proof. Omitted/exercise, 2.1.1 of Kuipers and Niederreiter. ■

For \sqrt{n} now.

$$S_N(c) = \#\{n \leq N : 0 \leq \{\sqrt{n}\} \leq c\}.$$

Note 1.36 If $d = \lfloor \sqrt{N} \rfloor$ then

$$\sqrt{n} = d + \{\sqrt{n}\}$$

and $d \leq \sqrt{n} \leq d + 1$ and $\#\{n : d \leq \sqrt{n} \leq d + 1\} = 2d + 2$.

Similarly

$$\#\{n : d \leq \sqrt{n} \leq d + \alpha\} = 2\alpha d + \alpha^2 + 1$$

then

$$\begin{aligned} S_N(\alpha) &= \sum_{j=0}^{\lfloor \sqrt{N} \rfloor} \#\{n : j + \alpha \leq \sqrt{n} \leq j + \alpha\} \\ &= \sum_{j=0}^{\lfloor \sqrt{N} \rfloor} (2\alpha j + \alpha^2 + 1) \\ &= 2\alpha \frac{\lfloor \sqrt{N} \rfloor (\lfloor \sqrt{N} \rfloor + 1)}{2} + O(\sqrt{N}) = \alpha N + O(\sqrt{N}) \end{aligned}$$

so

$$D_N^* = \sum_{0 \leq \alpha \leq 1} \left\| \frac{S_N(\alpha)}{N} - \alpha \right\| = \sup_{0 \leq \alpha \leq 1} O_\alpha(1/\sqrt{N}) = O(1/\sqrt{N}).$$

Exercise 1.37 Make the dependence on α explicit and make the proof rigorous.