Equidistribution in Number Theory

MA841 BU Fall 2018

Salim Ali Altuğ

September 11, 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 $N \to \infty$? □

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 $N \to \infty$, N squarefree $N \not\equiv 7 \pmod 8$, $\left(\frac{N}{p}\right) = 1$ for some fixed odd prime p*

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

where $\mathrm{d}\sigma$ 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

$$\pm\Gamma\backslash\mathbf{H}$$

$$\mathbf{H} = \left\{x + iy \in CC : y > 0\right\}$$

$$\Gamma = \mathrm{SL}_2(\mathbf{Z})$$

$$\mathcal{F} = \left\{z \in \mathbf{H} : -\frac{1}{2} \leq \Re(z) \leq 0, |z| \geq 1 \text{ or } \frac{1}{2} > \Re(z) > 0, |z| > 1\right\}$$

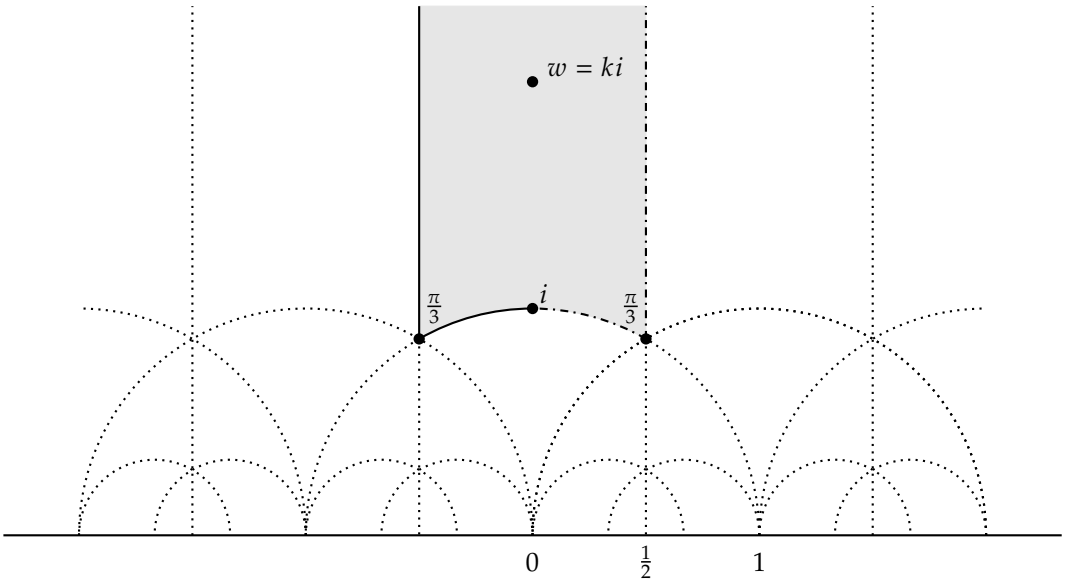

Figure 1.4: $\mathcal{F}$

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

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

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

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 $Q = a(x^2 + xy + y^2)$ $(d = -3)$. ◊

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

$$\mathrm{d}\mu = \frac{3}{\pi} \frac{\mathrm{d}x\, \mathrm{d}y}{y^2}.$$

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

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

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 $\left\{\frac{3}{2}\right\} = \frac{1}{2}$. 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. □

Example 1.11 If $\alpha = \sqrt{2}$ so $\{\alpha\} \approx 0.4142?\ldots$ $\{\alpha 2\} \approx 0.8284?\ldots$ $\{\alpha 3\} \approx 0.24264\ldots$ $\{\alpha 4\} \approx 0.656854\ldots$ 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 $b - a$. □

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 $q > 0$.*

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

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

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

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

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

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

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. ∎

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

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

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

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

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

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 $g > 0$*

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

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

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

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

$$\frac{f(p/q) - \cancelto{0}{f(\alpha)}}{p/q - \alpha} = f'(x_0)$$

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 $f \in \mathbf{Z}[x]$, e.g. elliptic curves with bounded integral discriminant)
- Roth ($\sim$ 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 $\alpha \notin \mathbf{Q}$.*

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

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

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 definie what is means to be uniformly distributed.

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

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

$\Diamond$

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.