Lecture 1

Some problems in number theory.

1. **Counting integral solutions.**

Consider a system of polynomial equations:

\[ X = \{ f_1(x_1, \ldots, x_d) = \ldots = f_n(x_1, \ldots, x_d) = 0 \}, \]

\[ f_1, \ldots, f_n \in \mathbb{Z}[x_1, \ldots, x_d] \]

Let \( N_T(X) = \# \{ x \in \mathbb{Z}^d : \max |x_i| \leq T \} \).

**Conj (Chambert-Loir, Tschinkel)**

For a "general class" of \( X \),

\[ N_T(X) \sim c \cdot T^a (\log T)^b \text{ as } T \to \infty, \]

for \( c > 0, a \in \mathbb{Q}^+, b \in \mathbb{N}_0 \).

\((a, b)\) are determined explicitly by geometry of \( X/\mathbb{Q} \).

II. Oppenheim Conj (1929)

\[ \mathbb{Q}(x_1, \ldots, x_d) = \mathbb{Q}(a_{ij} x_i x_j, a_{ij} \in \mathbb{R}) \]

Assume that:

- \( d \geq 3 \),
- \( \mathbb{Q} \) is nondegenerate ( \( \det(a_{ij}) \neq 0 \)),
- \( \mathbb{Q} \) is indefinite ( \( \mathbb{Q}(\mathbb{R}^d) = \mathbb{R} \)),
- \( \mathbb{Q} \) is irrational ( \( \mathbb{Q} \neq \alpha \cdot \mathbb{Q}_0 \) where \( \mathbb{Q}_0 \) has rational coefficients).

Then \( \mathbb{Q}(\mathbb{Z}^d) \) is dense in \( \mathbb{R} \).

Proved by Margulis in 1987.
Ex. \( \{ x^2 + y^2 - \sqrt{2} z^2 : x, y, z \in \mathbb{Z} \} \) is dense in \( \mathbb{R} \).

III. Littlewood Conjecture (1930)

For every \( \alpha, \beta \in \mathbb{R} \),

\[
\liminf_{n \to \infty} n \cdot d(n\alpha, \mathbb{Z}) \cdot d(n\beta, \mathbb{Z}) = 0
\]

Still Open?

IV. Diophantine approximation

Given \( x \in \mathbb{R}^d \), how well can we approximate \( x \) by rational vectors: \( x \sim \frac{p}{q} \).

Fix \( \psi : \mathbb{R}^+ \to \mathbb{R}^+ \).

The vector \( x \) is called \( \psi \)-approximable if

\[
\| x - \frac{p}{q} \| \leq \frac{\psi(q)}{q^\delta}
\]

has infinitely many solutions.

Thm. (Rhinchen - Geoshep)

"Typical" \( x \in \mathbb{R}^d \) are \( \psi \)-approximable

\[
\sum_{\ell=1}^{\infty} \psi(\ell)^d = \infty
\]

ex. For "typical" \( x \),

\[
\| x - \frac{p}{q} \| \leq q^{-1/2} \text{ has inf. many solutions,}
\]
but \( \| x - \frac{p}{q} \| < \frac{\epsilon}{q^{1 + \frac{1}{d}}} \), \( \epsilon > 0 \), only finitely many.

**Def.**

1) \( x \in \mathbb{R}^d \) is **badly approximable** if

\[
\exists \epsilon > 0: \forall p \in \mathbb{Z}^d \forall q \in \mathbb{N}, \quad \| x - \frac{p}{q} \| > \frac{\epsilon}{q^{1 + \frac{1}{d}}}.
\]

2) \( x \in \mathbb{R}^d \) is **well approximable** if for some \( \epsilon > 0 \),

\[
\| x - \frac{p}{q} \| \leq \frac{\epsilon}{q^{1 + \frac{1}{d} + \epsilon}}
\]

has infinitely many solutions.

\[\rightarrow\] The set of badly approximable vectors is a complicated fractal set.

\[\rightarrow\] "Typical" vectors in \( \mathbb{R}^d \) are not well approximable.

**Conj. (Sprindzuk; 1980)**

If \( X \) is a "curved" surface in \( \mathbb{R}^d \) then "typical" \( x \in X \)

is not well approximable.


---

**Introduction to dynamical systems.**

A dynamical system consists of a space \( X \), and a transformation \( T: X \rightarrow X \).

\[ T^0 \cdot T^1 \cdot T^2 \ldots \]

Orbit: \( \{ x, T^0 x, T^1 x, \ldots \} \)

**Basic problem**: Understand distribution of orbits:
given $A \subset X$, 
$\#\{i=0...N: \text{T}^i x \in A\} \overset{N \to \infty}{\to \infty}$

**Two Examples:**

$X = S' = \{ z \in \mathbb{C}: |z|=1 \}$. 

1) Rotation: 

$T_\alpha: S' \to S': z \mapsto e^{2\pi i \alpha} z$

2) Doubling: 

$D_2: S' \to S': z \mapsto z^2$.

**Def.** $T$ is called mixing if $\forall \psi_1, \psi_2: X \to \mathbb{C}$

$$\int_X \psi_1(T^n x) \psi_2(x) \, dx \to (\int_X \psi_1(x) \, dx) (\int_X \psi_2(x) \, dx) \quad (n \to \infty)$$

(compare with notion of independence in Probability: observables $\psi_1 \circ T^n$ and $\psi_2$ become asymptotically independent)

**Prop.** The doubling map $D_2: S' \to S'$ is mixing.

---

**Fourier analysis:**

First, consider $\psi_1(z) = z^n$, $\psi_2(z) = z^m$ - characters.

Recall that $\int_{S'} z^n \, dz = \begin{cases} 0, & n \neq 0, \\ 1, & n = 0. \end{cases}$

$$\int_{S'} \psi_1(D_2^n z) \psi_2(z) \, dz = \int_{S'} z^{2n_1 + n_2} \, dz = \begin{cases} 1, & n_1 = n_2 = 0, \\ 0, & n_1 \neq 0 \text{ or } n_2 \neq 0 \text{ and } n >> 0. \end{cases}$$
Hence, \[ \int_{S^1} (\varphi \circ T^n) \, d\mu \rightarrow (\int_{S^1} \varphi \, d\mu)^n \] for sufficiently large $n$.

Next, any continuous function on $S^1$ can be approximated by linear combinations of characters.

**Prop.** Let $x \in \mathbb{R}$. Then for every $x \in S^1$, interval $A \subset S^1$

\[
\frac{\#\{ i = 0, \ldots, N : T^n x \in A \}}{N+1} \rightarrow |A|.
\]

(in particular, every orbit is dense.)

We need to show that \( \frac{1}{N+1} \sum_{n=0}^N \chi_A (T^n x) \rightarrow \int_{S^1} \varphi \)

where \( \chi_A \) is the characteristic function of \( A \).

Approximate \( \chi_A \) by linear combinations of characters...

Then we need to show that

\[
\frac{1}{N+1} \sum_{n=0}^N \varphi (T^n x) \rightarrow \int_{S^1} \varphi
\]

for \( \varphi (z) = z^m \). For \( m \neq 0 \),

\[
\frac{1}{N+1} \sum_{n=0}^N (e^{2\pi i m x})^n = \frac{x^m}{N+1} \sum_{n=0}^N (e^{2\pi i m x})^n
\]

\[
= \frac{x^m}{N+1} \cdot \frac{(e^{2\pi i m x})^{N+1} - 1}{e^{2\pi i m x} - 1} \rightarrow 0,
\]

since \( e^{2\pi i m x} \neq 1 \).

\( \rightarrow \) "Typical" orbits of the doubling map \( D_2 \)

are dense in \( S^1 \), but there are many complicated orbits.
Theorem (Furstenberg) Let $p, q$ be primes, and $z \in \mathbb{Z}^d$. Then
\[ \{ P^m R^n z : m, n \geq 0 \} = S' \]
This property is related to the Littlewood Cayley space of lattices.

A lattice in $\mathbb{R}^d$ is a subgroup \( L = \mathbb{Z} v_1 + \ldots + \mathbb{Z} v_d \) for a basis\( \{ v_i \} \) of $\mathbb{R}^d$.

Let \( \mathcal{L}_d = \{ \text{set of all lattices in } \mathbb{R}^d \} \).
\( \mathcal{B}_d = \{ \text{set of all bases} \} = \{ (v_1, \ldots, v_d) \in \mathbb{R}^d : \det(v_1, \ldots, v_d) \neq 0 \} \)
\( (v_1, \ldots, v_d) \sim (v'_1, \ldots, v'_d) \) if \( \mathbb{Z} v_1 + \ldots + \mathbb{Z} v_d = \mathbb{Z} v'_1 + \ldots + \mathbb{Z} v'_d \).

Then \( \mathcal{L}_d \cong \mathcal{B}_d / \sim \).

\( G = \text{GL}_d(\mathbb{R}) = \{ g \in \text{Mat}_d(\mathbb{R}) : \det(g) \neq 0 \} \).
The group $G$ acts on $\mathcal{B}_d$ and $\mathcal{L}_d$:
\( \{ v_i \} \xmapsto{g} \{ v_i g \} \).
Note that $G$ acts transitively on $\mathcal{Bd}$ and $\mathcal{Ld}$. Let \{e_i\} be the standard basis.

If $g \cdot \{e_i\} = \{e_i\}$, then $g = \text{id}$, so that

$$\mathcal{Bd} \sim G\text{ld}(\mathbb{R}).$$

If $g \cdot (\mathbb{Z}e_1 + \ldots + \mathbb{Z}e_d) = \mathbb{Z}e_1 + \ldots + \mathbb{Z}e_d$, then

$g \in \text{Mat}_d(\mathbb{Z})$ and $g^{-1} \in \text{Mat}_d(\mathbb{Z})$

equivalently, $g \in \text{Mat}_d(\mathbb{Z})$ and $\det(g) = \pm 1$.

Converse also holds.

Hence, $\text{Stab}_G(\mathbb{Z}e_1 + \ldots + \mathbb{Z}e_d) = \{g \in \text{Mat}_d(\mathbb{Z}) : \det(g) = \pm 1\}$

and $\mathcal{Ld} \sim G\text{ld}(\mathbb{Z}) \setminus G\text{ld}(\mathbb{R})$.

The space $\mathcal{Ld}$ is equipped with natural topology and (finite, invariant) measure.

**Measure**

A measure $\mu$ on $X$ is a map $\mu : \{\text{subsets of } X\} \to [0, \infty)$ such that:

1) $\mu(\emptyset) = 0$

2) $\mu\left( \bigcup_{i \geq 1} A_i \right) = \sum_{i \geq 1} \mu(A_i)$ for every $A_i \in X$ such that $A_i \cap A_j = \emptyset$ for $i \neq j$.

In general, it is impossible to define $\mu$ on all subsets of $X$ consistently, but only on a "large"
family of subsets (called measurable subsets).

Alternatively, one can think of \( \mu \) as

\[ \mu : \{ \text{ functions } \} \rightarrow C. \]

ex. Lebesgue measure \( \lambda : \{ \text{ measurable subsets } \} \rightarrow \mathbb{R}^+ \cup \{0\} \)

\[ \lambda \left( \bigcap_{i=1}^{d} (a_i, b_i) \right) = \prod_{i=1}^{d} (b_i - a_i). \]

Invariant measure on \( GL_d(\mathbb{R}) \) (Haar measure)

**Thm**

\[ G = GL_d(\mathbb{R}). \text{ The measure } \mu \text{ defined by} \]

\[ \int_{G} f(g) \cdot \left( \prod_{i=1}^{d} dg_{ij} \right) \quad \text{det}(g)^{d-1} \]

is invariant under left/right multiplication.

(That is, \( \int_{G} f(gh) \mu(g) = \int_{G} f(g) \mu(g) \).

For \( g \in G \), the map \( h \mapsto gh = g \)

defines a differential transformation of \( \text{Mat}(\mathbb{R}) \)

with \( \text{Jac}(h \mapsto gh) = \text{det}(g)^{d-1}. \) Hence,

\[ \int_{G} f(g) \cdot \left( \prod_{i=1}^{d} dg_{ij} \right) \quad \text{det}(g)^{d-1} \]

\[ = \int_{G} f(gh) \cdot \text{Jac}(h \mapsto gh) \cdot \left( \prod_{i=1}^{d} dh_{ij} \right) \quad \text{det}(gh)^{d-1} \]

\[ = \int_{G} f(gh) \cdot \left( \prod_{i=1}^{d} dh_{ij} \right) \quad \text{det}(h)^{d-1}. \]

\[ \rightarrow \text{Invariant measures exist on every loc. compact group. Moreover, such measure is unique up to a scalar multiple.} \]