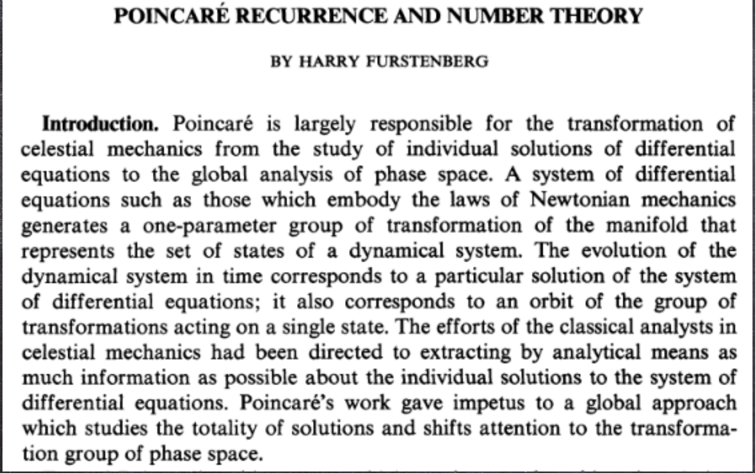
Las interacciones de la teoría ergódica y la teoría de números

Sebastián Donoso

Centro de Modelamiento Matemático & Departamento de Ingeniería Matemática
Universidad de Chile

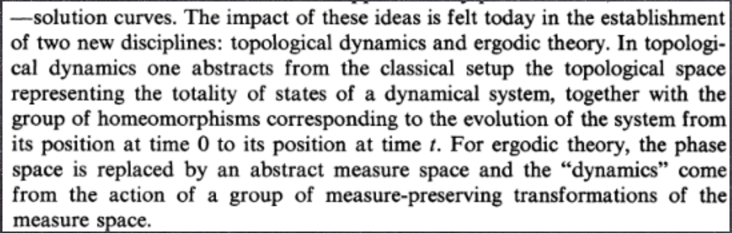
Seminario LATeN, 27 de abril, 2022



POINCARÉ RECURRENCE AND NUMBER THEORY

BY HARRY FURSTENBERG

Introduction. Poincaré is largely responsible for the transformation of celestial mechanics from the study of individual solutions of differential equations to the global analysis of phase space. A system of differential equations such as those which embody the laws of Newtonian mechanics generates a one-parameter group of transformation of the manifold that represents the set of states of a dynamical system. The evolution of the dynamical system in time corresponds to a particular solution of the system of differential equations; it also corresponds to an orbit of the group of transformations acting on a single state. The efforts of the classical analysts in celestial mechanics had been directed to extracting by analytical means as much information as possible about the individual solutions to the system of differential equations. Poincaré's work gave impetus to a global approach which studies the totality of solutions and shifts attention to the transformation group of phase space.



—solution curves. The impact of these ideas is felt today in the establishment of two new disciplines: topological dynamics and ergodic theory. In topological dynamics one abstracts from the classical setup the topological space representing the totality of states of a dynamical system, together with the group of homeomorphisms corresponding to the evolution of the system from its position at time 0 to its position at time t. For ergodic theory, the phase space is replaced by an abstract measure space and the "dynamics" come from the action of a group of measure-preserving transformations of the measure space.

Text extracted from *Poincaré recurrence and number theory* by H. Furstenberg (1981).

What is ergodic theory about?

Very roughly speaking one study the long term behavior of en evolving system.
In this talk the setting is:

- $(X, \mathcal{X}, \mu)$ is a probability space.

- $T\colon X \to X$ is a bi-measurable, measure preserving transformation. This means that $\mu(T^{-1}A) = \mu(A)$ for all $A \in \mathcal{X}$.

If I speak of several transformations $T_1, \ldots, T_d$ I mean that each one is measure preserving (as above).

Theorem (Poincaré recurrence theorem (1890))

Let $(X, \mathcal{X}, \mu, T)$ be a measure preserving system, and $A \in \mathcal{X}$, $\mu(A) > 0$. Then, there exists $n \in \mathbb{N} \setminus \{0\}$ such that $\mu(A \cap T^{-n}A) > 0$.

Formally proved by Carathéodory (1919) using measure theory

Some questions:

- Can be n chosen in a nice set? (for instance the square numbers).
- Multiple recurrence?
- Quantitative versions of recurrence?
- How about groups other than $(\mathbb{Z}, +)$

The ergodic theorem

Theorem (Von Neumann's Ergodic Theorem (1932))

Let $(X, \mathcal{X}, \mu, T)$ *be a measure preserving system and* $f \in L^2(\mu)$*. Then*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=0}^{N-1} f \circ T^n \to \mathbb{E}(f|\mathcal{I}(T)).$$

Theorem (Weak version)

Let $(X, \mathcal{X}, \mu, T)$ *be a measure preserving system and* $A \in \mathcal{X}$, $\mu(A) > 0$*. Then*

$$\lim_{n\to\infty} \frac{1}{n} \sum_{n=0}^{N-1} \mu(A \cap T^{-n}A) \geq \mu(A)^2.$$

Sets of recurrence

Definition

A subset $R \subseteq \mathbb{N}$ is a set of recurrence, if for any measure preserving system $(X, \mathcal{X}, \mu, T)$, and $\mu(A) > 0$, there exists $n \in R$ such that $\mu(A \cap T^{-n}A) > 0$.

Examples:

- $\mathbb{N} \setminus \{0\}$.
- For an infinite set A, the difference set $A - A = \{a - b : a, b \in A, a > b\}$.
- Shifted primes ($\mathbb{P} - 1$, $\mathbb{P} + 1$).
- $\{n^2 : n \in \mathbb{N}\} \setminus \{0\}$.
- $\{p(n) : n \in \mathbb{N}\} \setminus \{0\}$ where p is divisible.

More definitions (topological)

A topological dynamical system is a tuple (X, T) where:

- X is a compact metric space.
- $T \colon X \to X$ is a homeomorphism.
- The system (X, T) is minimal if all orbits are dense in X.

We can consider similar definitions for recurrence sets.

Definition

A subset $R \subseteq \mathbb{N}$ is a set of topological recurrence, if for any minimal (X, T), and any non-empty open set $U \subseteq X$, there exists $n \in R$ such that $U \cap T^{-n}U \neq \emptyset$.

Obs:

Recurrence $\overset{\Longrightarrow}{\not\Longleftarrow}$ Top. Recurrence

Dynamics and equations

Monochromatic solutions to some equation.

Theorem

- *A subset $R \subseteq \mathbb{N}$ is a set of recurrence iff for any positive density subset S of $\mathbb{N}$, there exist different $n, m \in E$ such that $n - m \in R$.*
- *A subset $R \subseteq \mathbb{N}$ is a set of topological recurrence iff for any coloring $\mathbb{N} = C_1 \cup \cdots \cup C_\ell$ of $\mathbb{N}$, there exist $n \neq m$ of the same color such that $n - m \in R$.*

Theorem (Furstenberg-Sárközy)

For any S of positive density, there exist different $n, m \in S$ such that $n - m$ is a perfect square.

Proof.

The set $R = \{k^2 : k \in \mathbb{N}\} \setminus \{0\}$ is a set of recurrence. □

The question of existence of (arbitrarily long) arithmetic progressions in certain subsets of integers has a long history.

van der Warden (1927) If we partition the naturals into finitely many colors, at least one of the subsets contains arbitrarily long arithmetic progressions.

Erdös and Turán (1936) conjectured it suffices to have positive *upper density*.

$$\overline{d}(E) = \limsup_{N\to\infty} \frac{1}{N} \left| E \cap [1, N] \right|$$

The question of existence of (arbitrarily long) arithmetic progressions in certain subsets of integers has a long history.

van der Warden (1927) If we partition the naturals into finitely many colors, at least one of the subsets contains arbitrarily long arithmetic progressions.

Erdös and Turán (1936) conjectured it suffices to have positive *upper density*.

$$\overline{d}(E) = \limsup_{N\to\infty} \frac{1}{N} \left| E \cap [1, N] \right|$$

Historical progress:

Roth (1952) : True for length 3 using Fourier analysis.

Szemerédi (1969) : True for length 4 combinatorial proof.

Szemerédi (1975) : True for arbitrary length! combinatorial proof.

Furstenberg (1977) : True for arbitrary length! using ergodic theory.

Fustenberg's proof initiated ergodic Ramsey theory: many applications to number theory and combinatorics.

A little about Furstenberg approach: connect the ergodic world with the combinatoric one via the Fustenberg correspondence principle.

Let E be a set of integers with positive upper density. There exist a measure preserving system $(X, \mathcal{X}, \mu, T)$ and a subset $A \subseteq X$ such that $\mu(A) = \overline{d}(E)$ and

$$\overline{d}((E+n_1) \cap (E+n_2) \cdots \cap (E+n_d)) \geq \mu(T^{-n_1}A \cap \cdots \cap T^{-n_d}A)$$

Note that

$$E \cap (E+n) \cap (E+2n) \cdots \cap (E+(d-1)n) \neq \emptyset$$

if and only if there exist

$$a \in E,\ a-n \in E,\ a-2n \in E,\ \ldots,\ a-(d-1)n \in E.$$

These points are in an arithmetic progression of lenght d.

So, in order to show that for some n

$$E \cap (E+n) \cap (E+2n) \cdots \cap (E+(d-1)n) \neq \emptyset$$

it suffices to show

$$\overline{d}(E \cap (E+n) \cap (E+2n) \cdots \cap (E+(d-1)n) > 0$$

and for this it suffices to show

$$\mu(A \cap T^{-n}A \cap T^{-2n}A \cdots \cap T^{-nd}A) > 0$$

This is the content of the Furstenberg multiple recurrence theorem (1977):

Theorem (Fustenberg (1977))

For every $(X, \mathcal{X}, \mu, T)$*, and every* $A \in \mathcal{X}$*,* $\mu(A) > 0$ *there exists* $n \in \mathbb{N}$ *such that*

$$\mu(A \cap T^{-n}A \cap T^{-2n}A \cdots \cap T^{-dn}A) > 0$$

Indeed he showed a stronger result:

Theorem (Fustenberg (1977))

for every $(X, \mathcal{X}, \mu, T)$*, and every* $A \in \mathcal{X}$*,* $\mu(A) > 0$ *we have*

$$\liminf_{N \to \infty} \frac{1}{N} \sum_{n=0}^{N-1} \mu(A \cap T^{-n}A \cap T^{-2n}A \cdots \cap T^{-dn}A) > 0$$

so there are many n's that work!

A glance at other questions/directions

Conjecture (Erdös-Graham (1980))

For any coloring $\mathbb{N} = C_1 \cup \cdots C_\ell$, there exist x, y, z of the same color such that $x^2 + y^2 = z^2$.

- It is not true for measure recurrence (i.e. asking in a positive density subset).
- M. Heule, O. Kullmann, and V. Marek (2016), true for 2 colors.

A glance at other questions/directions

Conjecture (Erdös-Graham (1980))

For any coloring $\mathbb{N} = C_1 \cup \cdots C_\ell$, there exist x, y, z of the same color such that $x^2 + y^2 = z^2$.

- It is not true for measure recurrence (i.e. asking in a positive density subset).
- M. Heule, O. Kullmann, and V. Marek (2016), true for 2 colors.

Conjecture (Erdös-Graham, relaxed version)

For any coloring $\mathbb{N} = C_1 \cup \cdots C_\ell$, there exist x, z of the same color such that $x^2 + y^2 = z^2$.

A glance at other questions/directions

Conjecture (Erdös-Graham (1980))

For any coloring $\mathbb{N} = C_1 \cup \cdots C_\ell$, there exist x, y, z of the same color such that $x^2 + y^2 = z^2$.

- It is not true for measure recurrence (i.e. asking in a positive density subset).
- M. Heule, O. Kullmann, and V. Marek (2016), true for 2 colors.

Conjecture (Erdös-Graham, relaxed version)

For any coloring $\mathbb{N} = C_1 \cup \cdots C_\ell$, there exist x, z of the same color such that $x^2 + y^2 = z^2$.

Pythagorean triples can be parametrized:
$x^2 + y^2 = z^2$ iff there exist n, m, k such that $x = k(n^2 - m^2)$, $y = 2knm$, $z = k(n^2 + m^2)$.

A glance at other questions/directions

Conjecture (Erdös-Graham (1980))

For any coloring $\mathbb{N} = C_1 \cup \cdots C_\ell$, there exist x, y, z of the same color such that $x^2 + y^2 = z^2$.

- It is not true for measure recurrence (i.e. asking in a positive density subset).
- M. Heule, O. Kullmann, and V. Marek (2016), true for 2 colors.

Conjecture (Erdös-Graham, relaxed version)

For any coloring $\mathbb{N} = C_1 \cup \cdots C_\ell$, there exist x, z of the same color such that $x^2 + y^2 = z^2$.

Pythagorean triples can be parametrized:
$x^2 + y^2 = z^2$ iff there exist n, m, k such that $x = k(n^2 - m^2)$, $y = 2knm$, $z = k(n^2 + m^2)$.
The points x, z are a Pythagorean pair iff

$$\frac{x}{z} = \frac{n^2 - m^2}{n^2 + m^2} \text{ for some } m, n.$$

Multiplicative actions

A multiplicative system is an action of the semigroup $(\mathbb{N}^*, \times)$.

Example:

$T_n \colon S^1 \to S^1$, $T_n(z) = z^n$ (or $x \mapsto x + \log(n)$) .

We may extend it to an action of $(\mathbb{Q}^{>0}, \times)$ if the transformations are invertible.

Multiplicative actions

A multiplicative system is an action of the semigroup $(\mathbb{N}^*, \times)$.

Example:

$T_n \colon S^1 \to S^1$, $T_n(z) = z^n$ (or $x \mapsto x + \log(n)$) .

We may extend it to an action of $(\mathbb{Q}^{>0}, \times)$ if the transformations are invertible.

Proposition

- *A subset $R \subseteq \mathbb{Q}^{>0}$ is a set of topological recurrence iff for any coloring $\mathbb{N} = C_1 \cup \cdots C_\ell$ there exist two elements $x \neq y$ of the same color such that $xz^{-1} \in R$.*
- *A subset $R \subseteq \mathbb{Q}^{>0}$ is a set of recurrence iff for any positive density of the same color such that $xz^{-1} \in R$*

Recall that $z^2 - x^2$ is a square number iff $xz^{-1} = \frac{n^2-m^2}{n^2+m^2}$. The combinatorial/number theoretical problem can be restated in dynamical terms:

Multiplicative actions

A multiplicative system is an action of the semigroup $(\mathbb{N}^*, \times)$.

Example:

$T_n \colon S^1 \to S^1$, $T_n(z) = z^n$ (or $x \mapsto x + \log(n)$) .

We may extend it to an action of $(\mathbb{Q}^{>0}, \times)$ if the transformations are invertible.

Proposition

- *A subset $R \subseteq \mathbb{Q}^{>0}$ is a set of topological recurrence iff for any coloring $\mathbb{N} = C_1 \cup \cdots C_\ell$ there exist two elements $x \neq y$ of the same color such that $xz^{-1} \in R$.*
- *A subset $R \subseteq \mathbb{Q}^{>0}$ is a set of recurrence iff for any positive density of the same color such that $xz^{-1} \in R$*

Recall that $z^2 - x^2$ is a square number iff $xz^{-1} = \frac{n^2-m^2}{n^2+m^2}$. The combinatorial/number theoretical problem can be restated in dynamical terms:

Question

Is the set $\left\{ \dfrac{n^2 - m^2}{n^2 + m^2} : n, m \in \mathbb{N} \right\}$ a set of (multiplicative) topological recurrence?

This approach was started by Frantzikinakis and Host.

Theorem (Frantzikinakis and Host (2013))

For $a, b, c, d \in \mathbb{Z}$, the set

$$\left\{\frac{(n+am)(n+bm)}{(n+cm)(n+dm)} : n, m \in \mathbb{N}\right\}$$

is a set of topological recurrence if $a \neq b$ y $c \neq d$.

Corollary

For any coloring of $\mathbb{N}$, there exist two distinct natural numbers x, y of the same color such that $16x^2 + 9y^2$ is a perfect square.

What they really showed is the following.

Theorem (Frantzikinakis and Host (2013))

Let $(X, \mathcal{X}, \mu, (T_n)_{n\in\mathbb{Q}^{>0}})$ *be a measure preserving system and* $A \in \mathcal{X}$, $\mu(A) > 0$. *Then*

$$\liminf_{N\to\infty} \frac{1}{N^2} \sum_{n,m\leq N} \mu(T^{-1}_{(n+cm)(n+dm)}A \cap T^{-1}_{(n+am)(n+bm)}A) > 0$$

Remark: if $a(n,m) = \frac{(n+am)(n+bm)}{(n+bm)(n+cm)}$, the expression above is equivalent to

$$\liminf_{N\to\infty} \frac{1}{N^2} \sum_{n,m\leq N} \mu(A \cap T^{-1}_{a(n,m)}A) > 0$$

Results of ergodic flavor

Definition (Subordinated semigroups)

We say that a semigroup $(\mathbb{N}^k, *)$ is *subordinated* to the Euclidean norm $\|\cdot\|$ in $\mathbb{N}^k$ if there exists a constant $C > 0$ such that

$$\|n * m\| \leq C\|n\|\|m\| \text{ for all } n, m \in \mathbb{N}^k. \tag{1}$$

Definition (Parametrized multiplicative function)

For $k \in \mathbb{N}$, we say that $f \colon \mathbb{N}^k \to \mathbb{Q}^{\geq 0}$ is a parametrized multiplicative function if there exists an operation $* \colon \mathbb{N}^k \times \mathbb{N}^k \to \mathbb{N}^k$ so that $(\mathbb{N}^k, *)$ is a semigroup subordinated to the euclidean norm in $\mathbb{N}^k$ and

$$f(n * m) = f(n)f(m)$$

for all $n, m \in \mathbb{N}^k$. We say that f is a *commutative parametrized multiplicative function* if one can choose $(\mathbb{N}^k, *)$ to be a cancelative commutative semigroup.

Theorem (D., Le, Moreira, Sun, (2021))

Let $(X, \mathcal{X}, \mu, T)$ be a measure preserving $(\mathbb{N}, \times)$-system and $A \in \mathcal{X}$ with $\mu(A) > 0$. Let $f\colon \mathbb{N}^k \to \mathbb{N}$ be a commutative parametrized multiplicative function and $\ell \in \mathbb{N}$. Then

$$\liminf_{N\to\infty} \mathbb{E}_{n\in[N]^k} \mu\Big(A \cap T_{f(n)}^{-1} A \cap T_{f(n)^2}^{-1} A \cap \cdots \cap T_{f(n)^\ell}^{-1} A\Big) > 0.$$

In particular,

$$\liminf_{N\to\infty} \frac{1}{N^2} \sum_{n,m\le N} \mu(A \cap T_{n^2+m^2}^{-1} A) > 0$$

or

$$\liminf_{N\to\infty} \frac{1}{N^2} \sum_{n,m\le N} \mu(A \cap T_{n^i m^j}^{-1} A) > 0$$

or even

$$\liminf_{N\to\infty} \frac{1}{N^2} \sum_{n_1,n_2,n_3,n_4\le N} \mu(A \cap T_{n_1^2+n_2^2+n_3^2+n_4^2}^{-1} A) > 0$$

More results on topological recurrence

Not much is known about sets of topological recurrence.

More results on topological recurrence

Not much is known about sets of topological recurrence.

Theorem (D., Le, Moreira, Sun, (2021))

For every $a, b \in \mathbb{N}$, $\{an + b : n \in \mathbb{N}\}$ *is a set of multiplicative recurrence if and only if* $a | b(b-1)$.

More results on topological recurrence

Not much is known about sets of topological recurrence.

Theorem (D., Le, Moreira, Sun, (2021))

For every $a, b \in \mathbb{N}$, $\{an + b : n \in \mathbb{N}\}$ is a set of multiplicative recurrence if and only if $a|b(b-1)$.

Theorem (D., Le, Moreira, Sun, (2021))

Let $a, c, \ell \in \mathbb{N}$, $b, d \in \mathbb{Z}$ and let $R := \left\{ \left(\frac{an+b}{cn+d}\right)^{\ell} : n \in \mathbb{N} \right\}$.

1) *If $a \neq c$, then R is not a set of topological multiplicative recurrence.*
2) *If $a = c$, $b \neq d$ and there exists a prime p such that $p|a$ but $p \nmid ,bd$, then R is not a set of topological multiplicative recurrence.*
3) *If $a = c$ and either $a|b$ or $a|d$, then R is a set of topological multiplicative recurrence.*

For example, for $a, k \in N^*$, $(an + k)/an$ is a set of topological recurrence.

Applications to number theory

Definition

A function $f\colon \mathbb{N}^* \to \mathbb{C}$ is called *completely multiplicative´* if $f(mn) = f(m)f(n)$ for $m, n \in \mathbb{N}^*$.

Theorem (O. Klurman and A. Mangerel. (2018))

Let f be a multiplicative function with $|f| = 1$. Then

$$\liminf_{n\to\infty} |f(n+1) - f(n)| = 0.$$

Theorem (D., Le, Moreira, Sun, (2021))

Let f be a multiplicative function with $|f| = 1$. Then for $a, k \in \mathbb{N}$,

$$\liminf_{n\to\infty} |f(an+k) - f(an)| = 0.$$

Proof idea.

Consider the topological $(\mathbb{N}, \times)$-system (S^1, T) where $S^1 = \{z \in \mathbb{C} : |z| = 1\}$ and $T_n e^{2\pi i x} = f(n) e^{2\pi i x}$ for all $x \in [0, 1)$ and $n \in \mathbb{N}$. Let $A = \{e^{2\pi i x} : x \in (-\epsilon/2, \epsilon/2)\} \subset S^1$. Use that $\frac{an+k}{an}$ is a set of topological recurrence. □

Questions

Question

Let $(X, \mathcal{B}, \mu, T)$ be a multiplicative measure preserving system and $A \in \mathcal{B}$ with $\mu(A) > 0$. Is it true that

$$\liminf_{N\to\infty} \mathbb{E}_{n,m\in[N]}\mu(T^{-1}_{n^2+m^2}A \cap T^{-1}_{m^2}A) > 0,$$

or

$$\liminf_{N\to\infty} \mathbb{E}_{n,m\in[N]}\mu(T^{-1}_{n^2+n}A \cap T^{-1}_{m^2}A) > 0?$$

We do not know whether $\{(6n+3)/(6n+2) : n \in \mathbb{N}\}$ is a set of topological multiplicative recurrence. Because of this reason, we ask:

Question

For $a \in \mathbb{N}$, $b, d \in \mathbb{Z}$, is it true that $S = \{(an+b)/(an+d) : n \in \mathbb{N}\}$ is a set of topological multiplicative recurrence if and only if $a|b$ or $a|d$?

Questions

Question

For which polynomial $P \in \mathbb{Z}[x]$ is $\{P(n) : n \in \mathbb{N}\}$ a set of topological multiplicative recurrence?

Even the answer for the following question is unknown:

Question

Is $\{n^2 + 1 : n \in \mathbb{N}\}$ a set of topological multiplicative recurrence?

Question

Are $\mathbb{P} - 1$ and $\mathbb{P} + 1$ sets of topological multiplicative recurrence?

Gracias!