Equidistribution and Related Topics

A course at the 2015 Ross Mathematics Program

Lectures by Vitaly Bergelson
Notes by Daniel Shapiro and Sohail Farhangi

Preface

This article is an expanded version of notes from a course by Vitaly Bergelson given at the *Ross Mathematics Program* during the six weeks of the summer of 2015. Daniel Shapiro worked with Bergelson to enhance and polish the notes taken by Sohail Farhangi during that class. We are grateful to Daniel Glasscock for his careful proofreading.

Contents

1 Denseness and Measure Zero **4**

1.1 Denseness 4

1.2 Measure 0 4

2 Uniform Distribution **6**

3 Denseness and Normal Numbers **8**

3.1 Normal Numbers 8

3.2 Denseness of $(n^k\alpha \mod 1)$ 9

3.3 Multiplicative Semigroups and Denseness mod 1 10

4 Uniform Distribution of Some Sequences **12**

4.1 Some Special Sequences 12

4.2 Sequences with 2 parameters 13

4.3 Aside: Cauchy's Functional Equation 13

5 Ultrafilters **15**

5.1 What is an Ultrafilter? 15

5.2 Generalizing Convergence 16

6 Notions of Largeness, and Well Distribution **18**

6.1 Largeness 18

6.2 Well Distribution 18

7 Topological Dynamical Systems **21**

7.1 Recurrence in Topological Dynamics 22

8 More on Topological Dynamics **23**

8.1 Symbolic Space 23

8.2 Isomorphic Topological Dynamical Systems 24

8.3 Aside: Poncelet's Porism 25

9 Measures and Normal Numbers **27**

9.1 Measures 27

9.2 More on Normal Sequences 29

10 Introduction to Ergodic Theory **31**

10.1 Measure Preserving Maps and the Ergodic Theorem 31

10.2 Poincaré Recurrence Theorem 34

10.3 Mixing 35

11 Varia **37**

11.1 Syndetic Sets 37

11.2 More on Poincaré Recurrence 38
11.3 {Squares} is a Set of Recurrence 39
11.4 Potpourri of Patterns in Primes and Ramsey Theory Connections 47

12 References **51**

1 Denseness and Measure Zero

1.1 Denseness

1.1 Definition. A set A is *dense* in $[0,1]$ if it is present in every sub-interval (a,b). That is, $A \cap (a,b) \neq \varnothing$ whenever $0 \leq a < b \leq 1$.

Trivially, $[0,1]$ and $(0,1)$ are each dense in $[0,1]$.
Easy exercise: $\mathbb{Q}$ and $[0,1] \setminus \mathbb{Q}$ are dense in $[0,1]$.

1.2 Definition. Suppose $\varepsilon > 0$. A set $A \subseteq [0,1]$ is *ε-dense* if every point $c \in [0,1]$ is within distance ε of some element of A. That is, for every $c \in [0,1]$ there exists $a \in A$ such that $|c-a| < \varepsilon$.

1.3 Exercise. Prove: Set A is dense in $[0,1]$ if and only if A is ε-dense in $[0,1]$ for every $\varepsilon > 0$.

1.4 Exercise. Define a *dyadic rational* to be a number of the form $\frac{m}{2^n}$ for integers n and m. Show that the dyadic rationals are dense in $[0,1]$. Can you generalize?

1.5 Definition. For a real number r, let $(r \mod 1) = r - \lfloor r \rfloor$. This is the "fractional part" of r.

1.6 Proposition. If the number α is irrational then the set $\{n\alpha \mod 1\}_{n=1}^{\infty}$ is dense in $[0,1]$.

Proof idea. Given any $\varepsilon > 0$ we want to show that this set is ε-dense. Choose integer N so that $0 < 1/N < \varepsilon$, and consider the N sub-intervals $I_j = (\frac{j}{N}, \frac{j+1}{N})$ with $0 \leq j < N$. By the pigeonhole principle, the values $(j\alpha \mod 1)$ for $1 \leq j \leq N+1$ cannot all be in different sub-intervals, so there exist $n_1 < n_2$ in $[1, N+1]$ such that $\big((n_2 - n_1)\alpha \mod 1\big)$ is within $1/N$ of 0. Then for $m = n_2 - n_1$ we have $(m\alpha \mod 1) \in (0, \frac{1}{N}) \cup (\frac{N-1}{N}, 1)$. Check that the set of numbers $(jm\alpha \mod 1)$ for $j = 1, 2, \ldots$ is ε-dense. [Consider two cases separately: $(jm \mod 1) \in (0, \frac{1}{N})$ and $(jm \mod 1) \in (1 - \frac{1}{N}, 1)$.] □

Remark. We often abuse terminology and say that a "sequence is dense" in an interval when we mean that the collection of terms in that sequence is a dense set in that interval. This is a minor point and shouldn't cause confusion.

1.7 Exercise. Suppose $a, b \in \mathbb{Q}$ and $a \neq 0$. If α is irrational, show that the sequence $\big((an+b)\alpha \mod 1\big)_{n=1}^{\infty}$ is dense in $[0,1]$.

1.8 Exercise. For irrational α, is the sequence $(n^2\alpha \mod 1)_{n=1}^{\infty}$ dense in $[0,1]$?
What about $(n^3\alpha \mod 1)_{n=1}^{\infty}$? Can you generalize?

This is a *very* challenging exercise! We will return to it later. See (3.13) and (4.2).

1.2 Measure 0

A set A of real numbers has measure zero if A can be covered by some collection of open intervals with arbitrarily small total length. That is:

1.9 Definition. A set $A \subset \mathbb{R}$ has *measure 0* if for every $\varepsilon > 0$, there exist intervals (a_n, b_n) for $n \in \mathbb{N}$, such that $A \subset \bigcup_{n \in \mathbb{N}} (a_n, b_n)$ and $\sum_{n \in \mathbb{N}} (b_n - a_n) < \varepsilon$. In this case we write $m(A) = 0$.

Claim. Every countable $S \subset \mathbb{R}$ has measure 0.
Proof. Let $(s_i)_{i=1}^{\infty}$ be an enumeration of the elements of S and let $\varepsilon > 0$ be given. To get a cover of total length $< \varepsilon$, use intervals $(s_i - \frac{1}{2^i}\frac{\varepsilon}{2}, s_i + \frac{1}{2^i}\frac{\varepsilon}{2})$ for $i = 1, 2, \ldots$. □

1.10 Exercise. If A is a set of measure 0, and $B \subset A$, show that B also has measure 0.

1.11 Exercise. The *Cantor set* is constructed from the interval $C_0 = [0,1]$ by an infinite process. For each $n \geq 0$, define C_{n+1} as the set obtained from C_n by removing the open middle third of each subinterval. For instance $C_1 = [0, 1/3] \cup [2/3, 1]$. The Cantor set C is the limit, that is $C = \bigcap_{n>0} C_n$.

Show that C is uncountable and has measure 0.
More on Cantor sets appears below in Exercise 9.9.

1.12 Exercise (Hard!)**.** Show that $[0,1]$ is not of measure 0.

For a property P, we say that P holds true for *almost every real number*, or that P holds true *almost everywhere* in $\mathbb{R}$, if the set $B = \{x \in \mathbb{R} : x \text{ does not satisfy } P\}$ has measure 0. For example, almost every real number is irrational.

Here is an interesting theorem that we will not prove here.

1.13 Theorem (Weyl)**.** Let $(n_k)_{k=1}^{\infty}$ be an increasing sequence of positive integers. For almost every real number α, the sequence $(n_k\alpha \mod 1)_{k=1}^{\infty}$ is dense in $[0,1]$.

1.14 Exercise. Show that there are uncountably many real numbers α such that the sequence $\{2^n\alpha \mod 1\}_{n=1}^{\infty}$ is not dense in $[0,1]$. [Hint. Consider binary expansions.]
Compare this result with the behavior of the sequence $(n\alpha)_{n=1}^{\infty}$ mentioned in Proposition 1.6.

Think about how you might define a notion of "measure zero" in $\mathbb{R}^d$.

In a different direction, how could we define "measure zero" subsets of $\mathbb{N}$? There are many valid possibilities, and we will encounter some of them later. One idea is to say that $S \subseteq \mathbb{N}$ is small if $\sum_{s\in S} \frac{1}{s}$ converges. Then the set of squares is small and the set of primes is not small.

Here's another quite different suggestion for a notion of smallness.

Let $A(m,b)$ denote the arithmetic progression $m\mathbb{N} + b$. This is the set of $n \in \mathbb{N}$ with $n \equiv b \pmod m$.

1.15 Definition. $S \subseteq \mathbb{N}$ is *AP-small* if for any $\varepsilon > 0$, there exist arithmetic progressions $A(m_k, b_k)$ for $k \in \mathbb{N}$, such that $S \subseteq \bigcup_{k\in\mathbb{N}} A(m_k, b_k)$ and $\sum_{k\in\mathbb{N}} \frac{1}{m_k} < \varepsilon$.

1.16 Exercise. Is $\mathbb{N}$ an AP-small set? (If the answer is "yes" then every subset S is AP-small.)

2 Uniform Distribution

2.1 Definition. A sequence $(x_n)_{n=1}^{\infty}$ in $[0,1]$ is *uniformly distributed* if for every $0 \le a < b \le 1$, we have:

$$\lim_{N\to\infty} \frac{|\{n \in [1,N] : x_n \in (a,b)\}|}{N} \;=\; b-a.$$

Uniform distribution depends on the order of the terms in the sequence, not just on the set of values. Denseness, on the other hand, depends only on the set and not on the order of the terms.

2.2 Exercise. Prove: A uniformly distributed sequence in $[0,1]$ must be dense in $[0,1]$.

2.3 Exercise. Suppose that $X = (x_n)_{n=1}^{\infty}$ in $[0,1]$ satisfies $\lim_{N\to\infty} \frac{|\{n \in [1,N] : x_n \in (a,b)\}|}{N} = b-a$ for every rational a and b with $0 \le a < b \le 1$. Show that X is uniformly distributed. What properties of the rationals were necessary for this exercise? Can you generalize?

It can be difficult to use the definition to determine whether a given sequence is uniformly distributed. It is often easier to use one of the following equivalent conditions for uniform distribution.

The first observation is that the fraction in (2.1) equals $\frac{1}{N}\sum_{n=1}^{N} f(x_n)$, where $f = 1_{(a,b)}$ is the "indicator function" for the subinterval (a,b).

2.4 Proposition. The sequence $(x_n)_{n=1}^{\infty}$ is uniformly distributed in $[0,1]$ if and only if for every continuous real valued function f defined on $[0,1]$:

$$\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} f(x_n) = \int_0^1 f(x)dx.$$

Hint for Proof: By definition, (x_n) is uniformly distributed in $[0,1]$ if and only if that limit condition holds true for every $f = 1_{(a,b)}$. Every continuous f can be approximated by a linear combination of such indicator functions. □

The condition in (2.4) for all continuous functions can be replaced by that condition just for the special functions $f(x) = x^k$ for $k \in \mathbb{N}$. This follows from the Weierstrass Approximation Theorem stated in (2.6) below. The trigonometric form of Weierstrass (see (2.7)) then yields the following simplified form of the criterion, first proved by Hermann Weyl [43] in 1916.

2.5 Proposition (Weyl's Criterion)**.** The sequence $(x_n)_{n=1}^{\infty}$ is uniformly distributed in $[0,1]$ if and only if for every positive integer h: $\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N} e^{2\pi i h x_n} \;=\; 0.$

Here are the analytic results used in the proof of Weyl's Criterion.

2.6 Theorem (Weierstrass Approximation Theorem)**.** For any real valued continuous function f on $[0,1]$, and any $\varepsilon > 0$, there exists a polynomial $p(x) \in \mathbb{R}[x]$ such that $\max_{x\in[0,1]} |f(x) - p(x)| < \varepsilon$.

Define a *trigonometric polynomial* to be a function of type $q(x) = a_0 + \sum_{n=1}^{N} \big(a_n \cos(2\pi n x) + b_n \sin(2\pi n x)\big)$, for some constants $a_j, b_j \in \mathbb{R}$. These functions have period 1, that is: $q(x+1) = q(x)$ for every $x \in \mathbb{R}$.

2.7 Theorem (Trigonometric Weierstrass)**.** For any real valued continuous function f on $[0,1]$ with $f(0) = f(1)$, and any $\varepsilon > 0$, there exists a trigonometric polynomial $q(x)$ such that $\max_{x\in[0,1]} \Big|f(x) - q(x)\Big| < \varepsilon$.

2.8 Definition. A metric space (X, d) is *separable* if it has a countable dense subset. For example, $[0,1]$ (with the usual metric) is separable.

2.9 Exercise. Let $C[0,1]$ be the set of continuous real valued functions on $[0,1]$, with the metric:

$$d(f,g) = \max_{x\in[0,1]} |f(x) - g(x)|.$$

Show: $C[0,1]$ is a separable metric space. [Hint: Consider the set of piecewise linear functions whose break-points are rational. Alternatively, use Weierstrass Approximation (2.6).]

2.10 Exercise. Prove that those two versions (2.6) and (2.7) of the Weierstrass Theorem are equivalent.

2.11 Exercise. Use the Trigonometric Weierstrass Theorem 2.7 to prove Weyl's Criterion 2.5.

Here's an illustration of the power of Weyl's Criterion.

2.12 Corollary. For irrational α, the sequence $(n\alpha \mod 1)_{n=1}^{\infty}$ is uniformly distributed in $[0,1]$.

Proof. For any $h > 0$ let $\lambda = e^{2\pi i h\alpha}$. Then $\lambda \neq 1$ since α is irrational, and:

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i h n\alpha} = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \lambda^n = \lim_{N\to\infty} \frac{1}{N} \frac{\lambda(\lambda^N - 1)}{\lambda - 1}.$$

Since $|\lambda| = 1$, the numerator is bounded and this limit is 0. Now invoke Weyl's Criterion 2.5. □

2.13 Exercise. Find an enumeration of $\mathbb{Q} \cap [0,1]$ that is not uniformly distributed.

2.14 Exercise. Show that the sequence $(\log n \mod 1)_{n=1}^{\infty}$ is dense in $[0,1]$, but not uniformly distributed.

2.15 Theorem (von Neumann [29])**.** If the sequence $X = (x_n)_{n=1}^{\infty} \subset [0,1]$ is dense, then there exists some re-numbering $\widetilde{X} = (\tilde{x}_n)_{n=1}^{\infty}$ of X, so that $\widetilde{X}$ is uniformly distributed.

Proof: Left as an exercise. [Hint. Choose a uniformly distributed sequence (a_n). For each n choose some x_k close to a_n. What about the unused x_k terms?] □

2.16 Definition. For $A \subset \mathbb{N}$, let $\overline{d}(A)$ denote its *upper density*. That is,

$$\overline{d}(A) \;=\; \limsup_{N\to\infty} \frac{|A \cap \{1, 2, \ldots, N\}|}{N}. \qquad (\star)$$

Similarly define the *lower density* $\underline{d}(A)$ by replacing the lim sup in $(\star)$ with lim inf. A set A has a **density** if $\overline{d}(A) = \underline{d}(A)$. Equivalently: A has density if the limit in $(\star)$ above exists. In that case we write $d(A)$ for the common value $\overline{d}(A) = \underline{d}(A)$.

2.17 Exercise. If $d(A)$ and $d(B)$ exist, then must $d(A \cup B)$ and $d(A \cap B)$ also exist?

2.18 Exercise. For an interval $[a,b] \subseteq [0,1]$ and a real number α, show that the density $d(S)$ exists for the set $S = \{n : (n\alpha \mod 1) \in [a,b]\}$. (Note: That set S might be empty!)

3 Denseness and Normal Numbers

3.1 Normal Numbers

A real number α can be written as an infinite decimal (in base ten notation). If that sequence of digits is sufficiently random, then each of the ten digits occurs with the same frequency. That is, for each digit d, the probability that d appears in the sequence is $1/10$. Each two-digit sequence should appear with probability $1/100$. Generally, each k-digit word (in the ten digit alphabet) should appear with probability 10^{-k}.

Are there any numbers α whose decimal digits exhibit such random behavior? Those sorts of questions can be investigated only after some precise definitions are made for terms like frequency, probability, and random.

Rather than using base ten, we concentrate on base 2 representations of a number. Parallel investigations for other bases are left as exercises.

3.1 Definition. Every $\alpha \in [0,1]$ has base 2 representation

$$\alpha = \sum_{n=1}^{\infty} \frac{a_n}{2^n} \quad \text{where } a_i \in \{0,1\}.$$

Some α's might have two binary representations. (Which ones?) In ambiguous cases we always choose the one ending with all zeros.

Define α to be *normal base* 2 if every finite 0-1 word of length k occurs in the binary sequence for α with frequency 2^{-k}. That is, $\alpha \in [0,1]$ is normal base 2 if, for any 0-1 word $W = (w_1, \ldots, w_k)$ of finite length k, we have:

$$\lim_{N\to\infty} \frac{\left|\{n \in [1,N] \ : \ a_{n+i} = w_i \ \ \forall\ 1 \le i \le k\}\right|}{N} \ = \ \frac{1}{2^k}.$$

More generally, α is normal base b if the base b representation contains every word of length k in the symbols $\{0, 1, \ldots, b-1\}$ appears with frequency b^{-k}. As an exercise, write out the more precise version of this definition.

Repeated coin tossing leads to a sequence of zeros and ones (interpreting tails as 0 and heads as 1, say). So a 0-1 sequence $(a_i)_{i=0}^{\infty}$ can be viewed as an infinite "coin tossing sequence." We do not attempt to provide a precise definition of "random," but we would expect that a sequence of random coin tosses will be normal. This idea is somewhat verified by the following famous result of Émil Borel, proved in 1909.

3.2 Theorem (E. Borel [9])**.** Almost all numbers in $[0,1]$ are normal base 2.

The same Theorem holds true for any integer base $b > 1$, not just for the case $b = 2$. Some discussion of the proof is presented in (10.12) below. This theorem is especially interesting because normal numbers are not easy to construct explicitly. In 1933 Champernowne [11] provided the first explicit construction of a number normal in base ten. His construction extends to other bases as well.

3.3 Exercise. Prove: Almost every real α is normal, meaning that α is normal in base b for every integer $b > 1$. [Assume Borel's Theorem for each base b.]

Another way to formulate Theorem 3.2 is to say: Almost every 0-1 sequence is normal. For that to make sense we need to know what "almost every" means in the space of binary sequences. That is, we need a notion of "measure zero" in the set C of all infinite 0-1 sequences $(a_i)_{i=1}^{\infty}$. One reasonable idea is to invoke the natural map $C \to [0,1]$ using binary representations:

$$(a_n)_{n=1}^{\infty} \text{ maps to } \alpha = \sum_{n=1}^{\infty} \frac{a_n}{2^n}.$$

Then a subset $S \subseteq C$ is defined to have measure zero if its image in $[0,1]$ has measure zero in the usual sense.

3.4 Exercise. The map $C \to [0,1]$ is not injective. For instance, sequences $01000\cdots$ and $00111\cdots$ yield same real number. Explain why this doesn't affect the definition of measure zero in the space C.
[Hint. Only countably many sequences exhibit that non-injective behavior.]
See the end of Section 8.1 below for a discussion of alternative approaches.

3.5 Exercise. $\alpha \in [0,1]$ is normal base 2 $\iff$ sequence $(2^n\alpha \mod 1)_{n=1}^{\infty}$ is uniformly distributed in $[0,1]$. More generally, α is normal base m exactly when $(m^n\alpha \mod 1)_{n=1}^{\infty}$ is uniformly distributed in $[0,1]$. (Compare Exercise 1.14.)

3.6 Exercise. List all finite words using an m-letter alphabet, and concatenate them into one infinite word. Show that this sequence is normal base m.

Note. No explicit example is known of a real number α that is normal in two different bases. Of course this depends on the definition of the word "explicit," since algorithms can be given that produce such numbers. On the other hand, almost every real number is normal for every base m, as seen in Exercise 3.3.

Many familiar numbers are conjectured to be normal, like $e, \pi, \ln 2$, and $\sqrt{2}$. But very little is known in that direction. For instance, no one can prove that the decimal expansion $\sqrt{2}$ contains infinitely many 3's (say).

3.2 Denseness of $(n^k\alpha \mod 1)$

In this section we outline a proof that:
For every irrational number α and positive integer k, the set $\{n^k\alpha \mod 1\}_{n=1}^{\infty}$ is dense in $[0,1]$.

In Proposition (1.6) we used the pigeonhole principle to prove the $k = 1$ case. For an approach to this result using uniform distribution, see Section 4.1 below.

The higher powers are trickier and require a more sophisticated version of pigeonholes. One method is to use van der Waerden's Theorem:

3.7 Theorem (van der Waerden)**.** Any finite coloring of $\mathbb{N}$ admits arbitrarily long, monochromatic arithmetic progressions.

It's useful to introduce a separate name for this property:

3.8 Definition. A set $S \subseteq \mathbb{N}$ is *AP-rich* if for every n the set S contains an arithmetic progression of length n.

With this terminology, Theorem 3.7 says:

$$\text{If } \mathbb{N} = \bigcup_{j=1}^{r} C_j \text{ is a finite union of subsets, then at least one of the } C_j\text{'s is AP-rich.}$$

Here we view that union as a coloring of the elements of $\mathbb{N}$. Elements of C_j are all the same color: that set is "monochromatic." Schur conjectured Theorem 3.7 around 1920, that conjecture was popularized by Baudet, and proved by van der Waerden in 1927. See [40] and [41] for the original proof. A somewhat different elementary proof is included in Khinchine's little book [25]. Some related results and generalizations are discussed in [21]. We will not present the proof in this course.

3.9 Exercise. (a) Must an AP-rich set contain infinitely many arithmetic progressions of given length n?
(b) Find an AP-rich set that contains no infinitely long arithmetic progression.

Van der Waerden's Theorem is a statement about equally spaced dots on a line. How can it be generalized to 2-dimensions? Working in $\mathbb{N}^2$ or $\mathbb{Z}^2$ (or in larger dimensions), we need to define an appropriate higher dimensional analogue of an arithmetic progression. One idea is to use equally spaced points in each direction, independently: an arithmetic progression of step-size d_1 in the x_1 direction, and a progression of step-size d_2 in the x_2 direction. (Here we index points in $\mathbb{Z}^2$ as (x_1, x_2) rather than the (x, y) used in high school calculus. Our notation is more natural for generalization to higher dimensions.)

3.10 Exercise. Use the classic van der Waerden Theorem (3.7) to prove:
Suppose $\mathbb{N}^2$ is finitely colored and $m \in \mathbb{N}$ is given. Then there exist $a = (a_1, a_2) \in \mathbb{N}^2$ and positive numbers d_1, d_2, such that the m^2 points $(a_1 + j_1 d_1, a_2 + j_2 d_2)$ for $0 \le j_1 < m$ and $0 \le j_2 < m$ all have the same color.

This says: For any finite coloring of $\mathbb{N}^2$, there exists some monochromatic rectangular grid. For our applications, we need the more difficult result: There exists a monochromatic *square* grid. That is, we change the statement in (3.10) by requiring $d_1 = d_2$.

3.11 Theorem (2-dimensional van der Waerden)**.** For any finite coloring of $\mathbb{N}^2$ and any positive integer m, there is a monochromatic $m \times m$ square. That is: there exists $(a_1, a_2) \in \mathbb{N}^2$ and a positive integer d such that all the points $(a_1 + j_1 d, a_2 + j_2 d)$ are assigned the same color, for $j_1, j_2 = 0, 1, \ldots, m-1$.

This theorem and its generalization to k dimensions was first proved by Tibor Gallai around 1943, but he apparently did not publish it. Gallai's Theorem is stated in Erdős's review of a paper by Richard Rado [34].

3.12 Exercise. Write out a statement of the k-dimensional van der Waerden Theorem.

Although this is a natural generalization of van der Waerden's Theorem the proof requires more sophisticated tools than what was used for the 1-dimensional case. And we didn't even prove that classic case in this short course! But we will point out how this combinatorial coloring theorem leads to a proof of the result we were hoping for.

3.13 Proposition. For any $k \in \mathbb{N}$ and any irrational α the set $\{n^k \alpha \mod 1\}_{n=1}^{\infty}$ is dense in $[0, 1]$.

Proof. We discuss the case $k = 2$ here. (For larger k, see Exercise 3.14.) Let $x_{nm} = (nm\alpha \mod 1)$ for $(n, m) \in \mathbb{N} \times \mathbb{N}$. Let $\varepsilon = 1/N$ be given and consider the partition of $[0, 1]$ into N subintervals $I_j = [\frac{j-1}{N}, \frac{j}{N}]$. We may disregard difficulties with endpoints of those intervals since α is irrational. Define an N-coloring χ of $\mathbb{N} \times \mathbb{N}$ by the rule: $\chi(n, m) = k$ if $x_{nm} \in I_k$. The 2-D van der Waerden Theorem (3.11) yields a monochromatic square (n_0, m_0), $(n_0 + d, m_0)$, $(n_0, m_0 + d)$, $(n_0 + d, m_0 + d)$. This means that all four of the numbers x_{nm} with indices being those pairs lie in the same subinterval I_k. Then they are all $\frac{1}{n}$-close to one another.

Now consider the following identity:

$$n_0 m_0 - (n_0 + d)m_0 - n_0(m_0 + d) + (n_0 + d)(m_0 + d) \;=\; d^2.$$

Multiply by $(\alpha \mod 1)$ and deduce that that $(d^2\alpha \mod 1)$ is $\frac{1}{N}$-close to either 0 or 1. [We get denominator N here rather than $4N$ because there are two plus terms and 2 minus terms.] Using that d, multiply by squares and examine the sequence $(m^2 d^2 \alpha \mod 1)$ for $m = 1, 2, \ldots$. Deduce that this sequence is $\frac{1}{\sqrt{N}}$-dense in $[0, 1]$. □

3.14 Exercise. For irrational α and any positive integer k, use the k-dimensional van der Waerden Theorem to prove that the set $\{n^k \alpha \mod 1\}$ is dense in $[0, 1]$.

3.3 Multiplicative Semigroups and Denseness mod 1

If α is irrational we know that the sequence $(n^k \alpha \mod 1)_{n \in \mathbb{N}}$ is dense in $[0, 1]$. (We will see later that this sequence is uniformly distributed.) Note that the set $G_k = \{n^k : n \in \mathbb{N}\}$ is a sub-semigroup of the

multiplicative semigroup $(\mathbb{N}, \cdot)$. It is interesting to ask whether similar density results also hold true for other sub-semigroups of $(\mathbb{N}, \cdot)$.

For a set $\mathcal{S} \subseteq \mathbb{N}$, we are considering the density mod 1 of the set $\mathcal{S}\alpha$. More precisely: Is $\{n\alpha \mod 1 : n \in \mathcal{S}\}$ dense in $[0,1]$?

3.15 Exercise. Suppose α is an irrational number.
(a) Show: $\mathcal{S}\alpha$ is dense mod 1, when $\mathcal{S}$ is the set of odd numbers. More generally, let $\mathcal{S}(k,m) = k + m\mathbb{N} = \{n \in \mathbb{N} : n \equiv k \pmod m\}$. Show that $\mathcal{S}(k,m)\alpha$ is dense mod 1.
(b) What if $\mathcal{S}$ is the set of 2-powers? Find irrational α such that $\{2^n\alpha \mod 1\}_{n=1}^{\infty}$ is not dense mod 1. Show that there are, in fact, uncountably many such α.

In light of (b) above, consider the larger set $\mathcal{S}_{2,3} = \{2^m 3^n : m, n \in \mathbb{N}\}$. Is $\mathcal{S}_{2,3}\alpha$ dense mod 1 ? Furstenberg answered this question in 1967.

3.16 Theorem (Furstenberg [18])**.** Suppose $x, y \in \mathbb{N}$ are multiplicatively independent (i.e. not powers of the same integer). Then for any irrational α, the set $\{x^m y^n \alpha \mod 1 \ : (m,n) \in \mathbb{N}^2\}$ is dense in $[0,1]$.
It follows that, if G is a sub-semigroup of $(\mathbb{N}, \cdot)$ with at least 2 generators, then $G\alpha = \{g\alpha \pmod 1\}_{g \in G}$ is dense in $[0,1]$.

3.17 Definition. A sequence of real numbers $(a_i)_{i=1}^{\infty}$ is *lacunary* if there is a constant $c > 1$ such that $\frac{a_{i+1}}{a_i} > c$ for every $i \geq 1$.

3.18 Exercise. Let $(x_i)_{i=1}^{\infty}$ be the sequence built by listing the set $\{2^m 3^n : (m,n) \in \mathbb{N}^2\}$ in increasing order.
(1) Show: $(x_i)_{i=1}^{\infty}$ is not lacunary. Moreover, $\lim\limits_{n\to\infty} \frac{x_{n+1}}{x_n} = 1$.
(2) In contrast to Theorem 3.16, prove that there is an irrational α such that the sequence $(x_i\alpha \mod 1)$ is not uniformly distributed in $[0,1]$. [Hint: Consider the base 6 representations.]

3.19 Remark. We can summarize the phenomena discussed above with an interesting dichotomy:

Let G be an infinite sub-semigroup of $(\mathbb{N}, \cdot)$ and list it as $G = \{x_1 < x_2 < \cdots\}$. Then:
either (i) G is *cyclic* in the sense that $G = \{c^n : n \geq n_0\}$ for some integers c, n_0 with $c > 1$;
or (ii) the elements x_n of G satisfy: $\frac{x_{n+1}}{x_n} \longrightarrow 1$.

In the first case, for almost all α the sequence $(c^n\alpha \mod 1)$ is u.d. (Compare Exercise 3.5.) On the other hand, there are uncountably many α for which $G\alpha \mod 1$ is not even dense.

In the second case, Furstenberg's Theorem 3.16 implies that $G\alpha \mod 1$ is dense for any irrational α.

4 Uniform Distribution of Some Sequences

4.1 Some Special Sequences

We mentioned that the set $\{n^k\alpha \mod 1\}_{n=1}^{\infty}$ is dense in $[0,1]$, whenever α is irrational. With some further work one can prove a stronger result:

The sequence $(n^k\alpha \mod 1)_{n=1}^{\infty}$ is uniformly distributed in $[0,1]$.

A natural question is: Which polynomials $p(x) \in \mathbb{R}[x]$ have the property that $(p(n) \mod 1)_{n=1}^{\infty}$ is dense in $[0,1]$? Or is uniformly distributed? The following Theorem, proved by Johannes van der Corput in 1931, will help us to answer this question.

4.1 Theorem (van der Corput)**.** Let $X = (x_n)_{n=1}^{\infty}$ be a sequence in $[0,1]$. For each positive integer h, assume that the sequence of differences $(x_{n+h} - x_n \mod 1)_{n=1}^{\infty}$ is uniformly distributed in $[0,1]$. Then X is uniformly distributed in $[0,1]$.

The proof is omitted. See [27], Chapter 1, §3 for further details. An extension is mentioned in (11.27) below. Also see the survey paper [8].

That sequence of differences is an analogue of the derivative: It is an operation that reduces "complexity." Note that the converse of Theorem 4.1 is not always true, as seen by considering $(n\alpha \mod 1)_{n=1}^{\infty}$.

4.2 Exercise. (1) For irrational α and fixed positive integer k, prove: $(n^k\alpha \mod 1)_{n=1}^{\infty}$ is uniformly distributed in $[0,1]$. [Assume Theorem (4.1).]

(2) More generally, let $p(x) \in \mathbb{R}[x]$ be a non-constant polynomial. Prove: $(p(n) \mod 1)_{n=1}^{\infty}$ is dense (or even uniformly distributed) in $[0,1]$ if and only if for some $j > 0$, the coefficient of x^j in $p(x)$ is irrational.

4.3 Exercise. Find a countable set X that is not dense in $[0,1]$, such that $X - X = \{a - b \mod 1 \mid a, b \in X\}$ is dense in $[0,1]$.

Another sequence of interest is $(n^c \mod 1)_{n=1}^{\infty}$, where $c > 0$ is not an integer.

4.4 Exercise. If $c \in (0,1)$ then the sequence $(n^c \mod 1)_{n=1}^{\infty}$ is dense in $[0,1]$.

[Outline of proof. For a sub-interval (a,b), there exists $N > 0$ such that $(n+1)^c - n^c < b - a$ for all $n \geq N$. However, the sequence $\sum_{k=0}^{n-1} (k+1)^c - k^c = n^c$ diverges. Since the step size between consecutive terms becomes arbitrarily small, the sequence $(n^c \mod 1)$ must be present in (a,b).]

4.5 Exercise. (a) Let $H_n = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$. Show: $(H_n \mod 1)_{n=1}^{\infty}$ is dense in $[0,1]$.
(b) For $c > 0$ show that $(\log^c(n) \mod 1)_{n=1}^{\infty}$ is dense in $[0,1]$.

The examples in the preceding two exercises show that denseness can be proved by knowing that the sequence grows slowly, without needing much detail about individual terms of the sequence.

Actually, the sequence $(n^c \mod 1)$ is uniformly distributed! This stronger result is proved by means of a theorem due to Lipót Fejér. (Fejér was thesis advisor of several famous Hungarian mathematicians, including von Neumann, Erdős, Pólya, and Turán.)

4.6 Theorem (Fejér)**.** Suppose f is a monotone differentiable function such that $\lim_{t\to\infty} f(t) = \infty$, $\lim_{t\to\infty} f'(t) = 0$, and $\lim_{t\to\infty} tf'(t) = \infty$. Then $(f(n) \mod 1)_{n=1}^{\infty}$ is uniformly distributed in $[0,1]$.

Fejér didn't publish a proof of this result, but see [27] Corollary 2.1 (page 14) for details of the argument. We mention Fejér's Theorem without proof because it leads to some interesting examples.

4.7 Exercise. Prove: For non-integer $c > 0$, the sequence $(n^c \mod 1)$ is uniformly distributed in $[0, 1]$.
[Hint. Use van der Corput Theorem 4.1 to reduce to the case $c \in (0, 1)$. Then apply Fejér's Theorem 4.6.]

4.8 Exercise. Define a "generalized polynomial" to be a finite $\mathbb{R}$-linear combination of real powers of x (not assuming integer exponents). Which generalized polynomials $p(x)$ satisfy the property that $(p(n) \mod 1)_{n=1}^{\infty}$ is uniformly distributed in $[0, 1]$?
Does your answer change if we require only denseness instead of uniform distribution?

4.9 Exercise. For $m \in \mathbb{N}$, define a notion of uniform distribution in an interval $[0, m]$. Show that the sequence $(n^k \alpha \mod m)_{n=1}^{\infty}$ is uniformly distributed in $[0, m]$.
[Hint. Compare this with uniform distribution of $(n^k \frac{\alpha}{m} \mod 1)_{n=1}^{\infty}$.]
How do these ideas generalize?

4.2 Sequences with 2 parameters

If α is irrational, then certainly the sequence $\big((m + n)\alpha \mod 1\big)$ (for $n, m \in \mathbb{N}$) is dense in $[0, 1]$. But is this 2-parameter sequence uniformly distributed in $[0, 1]$ in some sense? Similarly, what about the sequence $(mn\alpha \mod 1)$? This discussion requires an extension of familiar definitions to sequences with two indices.

4.10 Definition. For a doubly-indexed sequence $X = (x_{n,m})_{(n,m)\in\mathbb{N}^2}$, define X to be *uniformly distributed as a 2-parameter sequence* in $[0, 1]$ if:

$$\lim_{N\to\infty} \frac{\big|\{(n, m) \ : \ 1 \le n, m \le N \text{ and } x_{n,m} \in (a, b)\}\big|}{N^2} \ = \ b - a.$$

Alternatively, we might say that X is uniformly distributed as a 2-parameter sequence in $[0, 1]$ if:

$$\lim_{N\to\infty} \frac{\big|\{(n, m) \ : \ n^2 + m^2 \le N^2 \text{ and } x_{n,m} \in (a, b)\}\big|}{\frac{\pi}{4}N^2} \ = \ b - a.$$

Examples. It turns out that both 2-parameter sequences $\big((n+m)\alpha \mod 1\big)_{(n,m)\in\mathbb{N}^2}$ and $(mn\alpha \mod 1)_{(n,m)\in\mathbb{N}^2}$ are uniformly distributed in $[0, 1]$, for either of those notions of uniform distribution of 2-parameter sequences.

4.11 Questions. (1) Are these two definitions equivalent, or do they lead to distinct notions of uniform distribution? You might also investigate some other ways that (n, m) might approach ∞.

(2) How would you define uniform distribution for a sequence in the unit square, that is for $(x_n)_{n=1}^{\infty}$ where $x_n \in [0, 1] \times [0, 1]$ (or in $\mathbb{T}^2$)?

4.3 Aside: Cauchy's Functional Equation

We digress from our main topic to make a remark about a famous old problem. While this problem is not directly related to uniform distribution, it contains useful ideas, some of which we refer to later.

What functions f from $\mathbb{R}$ to $\mathbb{R}$ satisfy: $f(x + y) = f(x) + f(y)$ for every $x, y \in \mathbb{R}$. This is known as *Cauchy's functional equation.*

Certainly for any $c \in \mathbb{R}$, $f_c(x) = cx$ is a solution to Cauchy's equation.

4.12 Exercise. If f satisfies Cauchy's equation, show that $f(rx) = rf(x)$ for every rational number r and every $x \in \mathbb{R}$. Therefore $c = f(1)$ satisfies: $f(r) = cr$ for every $r \in \mathbb{Q}$.
If f is continuous, show that $f = f_c$, for some c. What if f is assumed only to be monotone? Or assumed only to be bounded on $[0, 1]$?
(It turns out that even those mild restrictions on f imply that $f = f_c$.)

It's surprising that there are many other functions that satisfy Cauchy's equation! To prove existence of non-standard solutions we need the following theorem from linear algebra.

4.13 Theorem. Every vector space has a basis.

Proof outline. Suppose V is a vector space over field F. The set of F-linearly independent subsets of V is partially ordered by inclusion. Show that every chain has an upper bound (the union). Zorn's Lemma implies existence of a maximal F-linearly independent set S of V. If S does not span V then exists $v \in V$ such that $S \cup \{v\}$ is F-linearly independent, contrary to maximality. Therefore S is a basis. □

4.14 Definition. A *Hamel basis* is a basis of $\mathbb{R}$ as a vector space over $\mathbb{Q}$.

Such a basis S does exist (by Theorem 4.13), but there is no reasonable way to write down its elements. A map $f : \mathbb{R} \to \mathbb{R}$ satisfies Cauchy's equation if and only if f is $\mathbb{Q}$-linear. Any choices of values of $f(s)$ for s in a Hamel basis S will extend to such a linear map. For instance, there is a Hamel basis S containing 1, and there exists f with $f(1) = 1$ and $f(s) = 0$ for all the other elements $s \in S$. Such f is not of the form f_c for any $c \in \mathbb{R}$.

4.15 Exercise. If f is a solution to Cauchy's functional equation and f is not of the form f_c, show that the graph of $y = f(x)$ is dense in the plane $\mathbb{R}^2$. (It's hard to draw that graph!)

5 Ultrafilters

5.1 What is an Ultrafilter?

Let's introduce a way to classify sets as large or small. We stick to a narrow meaning of those words, allowing no other choices: *every* set is either large or small. No set can be both large and small.

To avoid set-theoretic contradictions we restrict attention to subsets of a given infinite set Ω. (Most often we'll just use $\Omega = \mathbb{N}$.) "Largeness" and "smallness" should satisfy the following simple rules. Here A and B are subsets of Ω. We write A^c for the complement of A, that is $A^c = \{x \in \Omega : x \notin A\}$.

1. Ω is large; $\varnothing$ is small.
2. A is large $\iff$ A^c is small.
3. If A has a large subset, then A is large.
4. If both A and B are large, then $A \cap B$ is large.
5. If $A \cup B$ is large, then A is large or B is large.
6. Every subset of a small set is small.
7. If $A \cap B$ is small, then A or B must be small.
8. If both A and B are small, then $A \cup B$ is small.

5.1 Exercise. Simplify the set of properties to eliminate implications among them.
Define "large" to mean infinite: Which properties above are violated?
Define "small" to mean finite (so "large" means cofinite). Which rules fail?

We may view this idea of largeness as a (finitely additive) measure p defined on the power set $\mathcal{P}(\Omega)$. [Recall that $\mathcal{P}(\Omega)$ is the collection of all subsets of Ω, so that $A \in \mathcal{P}(\Omega)$ means $A \subseteq \Omega$.]
This measure takes on only two values, recording whether a set is small or large. Here are basic properties:

$p : \mathcal{P}(\Omega) \to \{0, 1\}$.
$p(\Omega) = 1$.
If $A, B \in \mathcal{P}(\Omega)$ are disjoint then $p(A \cup B) = p(A) + p(B)$.

A measure p with those three properties is called an ultrafilter.

5.2 Definition. An *ultrafilter* on Ω is a finitely additive, $\{0, 1\}$-valued measure on $\mathcal{P}(\Omega)$.

5.3 Exercise. If p is an ultrafilter, define set A to be p-large if $p(A) = 1$. Define A to be p-small if A^c is p-large. Verify the 8 properties listed above.

Example. Choose $c \in \Omega$, and declare $p_c(A) = 1$ if and only if $c \in A$. Check that p_c is an ultrafilter, and that a set if p_c-large iff it contains c. Such (somewhat trivial) examples are called the *principal ultrafilters.*

5.4 Exercise. If Ω is finite, show that every ultrafilter on Ω is principal.
(Generally, ultrafilter p is principal if and only if there is a p-large finite set.)

Before discussing uses of ultrafilters, let's verify that some non-trivial examples exist.

5.5 Definition. A *filter* $\mathcal{F}$ on Ω is a non-empty collection of subsets of Ω satisfying:

1. Closed under finite intersection: if $A, B \in \mathcal{F}$ then $A \cap B \in \mathcal{F}$.
2. Closed under superset: if $A \in \mathcal{F}$ and $A \subseteq B$ then $B \in \mathcal{F}$.
3. Nontriviality: $\varnothing \notin \mathcal{F}$.

5.6 Exercise. Suppose $\mathcal{F}$ is a filter on Ω and define a set $A \subseteq \Omega$ to be $\mathcal{F}$-large if $A \in \mathcal{F}$. Define A to be $\mathcal{F}$-small if A^c is $\mathcal{F}$-large. Which of the eight properties above does this notion of largeness satisfy?

If Ω is infinite, let $\mathcal{F}_0$ be the collection of subsets of Ω that are cofinite (those whose complements are finite). Verify that $\mathcal{F}_0$ is a filter.

If $\mathcal{F}$ is a filter, then $\mathcal{F}$ is contained in a maximal filter. This follows by applying Zorn's Lemma to the collection of filters that contain $\mathcal{F}$, ordered by inclusion.

5.7 Exercise. Suppose $\mathcal{U}$ is a maximal filter on Ω.
(1) Prove: For any $A \subseteq \Omega$, either $A \in \mathcal{U}$ or $A^c \in \mathcal{U}$.
(2) Define $p : \mathcal{P}(\Omega) \to \{0, 1\}$ by: $p(A) = 1$ if $A \in \mathcal{U}$ and 0 otherwise. Prove: p is an ultrafilter.
(3) If p is an ultrafilter on Ω, let $\mathcal{U}$ be the set of A with $p(A) = 1$. Show: $\mathcal{U}$ is a maximal filter.

Exercise 5.7 verifies that an *ultrafilter* is a maximal filter. Moreover, this approach leads to a proof that non-principal ultrafilters exist.

5.8 Exercise. If Ω is infinite, there exists a non-principal ultrafilter on Ω.
[Hint. A maximal filter containing $\mathcal{F}_0$ cannot be principal.]

5.2 Generalizing Convergence

Ultrafilters provide an efficient way to generalize the definition of the limit of a sequence. For a sequence (x_n) of real numbers, recall that $\lim_{n\to\infty} x_n = L$ means:

For every $\varepsilon > 0$, there exists N such that $|x_n - L| < \varepsilon$ whenever $n > N$.

Equivalently: Given $\varepsilon > 0$, the set of indices n such that $|x_n - L| < \varepsilon$ is cofinite.

Rather than using the filter $\mathcal{F}_0$ of cofinite sets in $\mathbb{N}$, we can use an ultrafilter p instead. The new definition for the limit to be L is: For $\varepsilon > 0$, the set $\{n \in \mathbb{N} \mid |x_n - L| < \varepsilon\}$ is p-large. With such a definition we find that limits exist much more often, but the limit value might depend on the choice of ultrafilter p.

For historical reasons, we use the letter p to denote a non-principal ultrafilter on $\mathbb{N}$. (Rather than calling the ultrafilter $\mathcal{U}$ as above.) We continue this notation for the rest of our course.

For $A \subseteq \mathbb{N}$, the statement $A \in p$ is equivalent to saying A is p-large.
Here is that limit definition generalized to metric spaces.

5.9 Definition. Suppose $(x_n)_{n=1}^{\infty}$ is a sequence in a metric space (X, d), and $y \in X$. Then $y = p\text{-}\lim_{n\to\infty} x_n$, that is, y is the p-limit of (x_n), if for every $\varepsilon > 0$, x_n is ε-close to y for a p-large set of indices n.
More precisely: If $\varepsilon > 0$, then $\{n \in \mathbb{N} \mid d(x_n, y) < \varepsilon\} \in p$.

5.10 Lemma. Suppose (X, d) is a metric space.

(1) If $\lim_{n\to\infty} x_n = y$ in X, then: $p\text{-}\lim_{n\to\infty} x_n = y$ for every non-principal ultrafilter p.

(2) If (x_n) is a sequence in X, and if both y and y' satisfy the definition of $p\text{-}\lim_{n\to\infty} x_n$, then $y = y'$.
[Uniqueness of p-limits]

Proof idea. (1) A cofinite set is p-large for every non-principal p.
(2) If $y \neq y'$ choose $0 < \varepsilon < \frac{1}{2}d(y, y')$. No x can be ε-close to both y and y'. Further details are left as an exercise. □

If X is a compact metric space, it's well known that any infinite sequence in X has a convergent subsequence. A non-convergent sequence in X might have many limit points (limits of various subsequences). This ambiguity of multiple limit points of a sequence disappears when using p-limits!

5.11 Lemma. For every ultrafilter p and compact metric space (X, d), every infinite sequence in X has a p-limit.

Proof outline. Suppose $(x_n)_{n=1}^{\infty}$ is a sequence in X but $p\text{-lim}\, x_n$ does not exist. Then for each $y \in X$ there exists $\varepsilon(y) > 0$ such that the set $A(y) = \{n \in \mathbb{N} \mid x_n \text{ is } \varepsilon(y)\text{-close to } y\}$ is p-small. Let $B(y)$ be the open ball about y of that radius $\varepsilon(y)$, so that $A(y) = \{n \in \mathbb{N} \mid x_n \in B(y)\}$. Compactness implies that some finite list $B(y_1), \ldots, B(y_m)$ cover X. But then $A(y_1) \cup \cdots \cup A(y_m) = \mathbb{N}$ so one of the $A(y_j)$ must by p-large. Contradiction. □

5.12 Exercise. If (x_n) does not converge (in the classical sense), then different ultrafilters p might yield different p-limits. Given a sequence (x_n) in a metric space (X, d), what values x can arise as $p\text{-lim}\, x_n$ for some ultrafilter p?

Ultrafilters are nice, but some are nicer than others. The "idempotent" ones are particularly useful. Before writing the definition, let's recall how to shift a set in $\mathbb{N}$. If $A \subseteq \mathbb{N}$ and $n \in \mathbb{N}$ we define $A - n = \{a - n : a \in A\}$. This is the left shift of A by n steps. Note that: $m \in A - n \iff m + n \in A$.

5.13 Definition. An ultrafilter p is *idempotent* if: $A \in p \iff \{n : A - n \in p\} \in p$.

In words, p is idempotent if: For any p-large A, p-many shifts of A are p-large.

The existence of idempotent ultrafilters on $\mathbb{N}$ follows by applying the following lemma to $\beta\mathbb{N}$, the set of all ultrafilters of $\mathbb{N}$. The tricky part is to define a type of product of ultrafilters to make $\beta\mathbb{N}$ into a semigroup.

5.14 Lemma (Ellis)**.** Any compact semi-topological semigroup contains an idempotent element.

This lemma, due to R. Ellis in 1958, is a direct application of Zorn's Lemma. See [15] and [3]. We skip the details here and assume that idempotent ultrafilters exist. The usefulness of idempotent ultrafilters is illustrated by the following wonderful limit property.

5.15 Proposition. Suppose X is a compact metric space and $(x_n)_{n=1}^{\infty}$ is a sequence in X. If p is an idempotent ultrafilter on $\mathbb{N}$, then $\underset{n\to\infty}{p\text{-lim}}\, x_n = \underset{m\to\infty}{p\text{-lim}} \big(\underset{n\to\infty}{p\text{-lim}}\, x_{n+m} \big)$.

This result is not hard to prove from the definitions, but (as usual for tangential topics) we omit details here, [they are presented in [3]]. This Proposition will be applied below in Theorem 7.14.

5.16 Exercise. Prove the converse of Proposition 5.15. That is, if p is an ultrafilter with that "lim-lim property," then p is idempotent. [This proof is somewhat tricky. Consider the sequence (n) in $\beta\mathbb{N}$.]

6 Notions of Largeness, and Well Distribution

6.1 Largeness

Last time we talked about measuring "largeness" of a subset of an infinite set Ω. For a given notion of largeness, let $\mathcal{L}$ be the collection of large subsets of Ω. What general properties should such a collection $\mathcal{L}$ have? Certainly we would insist on a few basic properties:

(1) $\Omega \in \mathcal{L}$; $\quad \varnothing \notin \mathcal{L}$.

(2) If $A \in \mathcal{L}$ and $A \subseteq B$, then $B \in \mathcal{L}$.

(3) If $A \cup B \in \mathcal{L}$, then $A \in \mathcal{L}$ or $B \in \mathcal{L}$.

Those rules provide a weak notion of "largeness." We sometimes encounter measures of size that enjoy additional properties. Two such properties come to mind:

(4) If $A \in \mathcal{L}$ then $A^c \notin \mathcal{L}$. [Notation: A^c is the complement of A.]

(5) If $A, B \in \mathcal{L}$, then $A \cap B \in \mathcal{L}$.

6.1 Exercise. Are properties (4) and (5) equivalent? [Prove (5) $\Rightarrow$ (4). Does the converse fail?]

6.2 Exercise. Suppose $\mathcal{L}$ satisfies properties (1), (2), (3), and let $\mathcal{F} = \{A \subseteq \Omega \mid A^c \notin \mathcal{L}\}$.
Is $\mathcal{F}$ a filter? Conversely, does a given filter $\mathcal{F}$ yield a corresponding $\mathcal{L}$?

6.3 Exercise. A collection $\mathcal{L}$ of subsets of Ω defines "largeness" if it satisfies properties (1), (2), and (3). We say that $\mathcal{L}$ defines "super-largeness" if it satisfies (1), (2), (3), (4), and (5).

Which of the following yields a notion of largeness? Which defines a notion of super-largeness?

(a) $A \subseteq \mathbb{N}$ is large if it is infinite.

(b) $A \subseteq \mathbb{N}$ is large if it is cofinite (its complement A^c is finite).

(c) $A \subseteq \mathbb{R}$ is large if it has positive Lebesgue measure.

(d) $A \subseteq \mathbb{R}$ is large if it is conull (A^c has measure zero).

(e) $A \subseteq \mathbb{N}$ is large if it has positive upper density. (See (2.16) for definition.)

(f) $A \subseteq \mathbb{N}$ is large if it has density 1.

(g) Subset A is large if it is p-large (relative to a given ultrafilter p).

(h) $A \subseteq \mathbb{N}$ is large if it is AP-rich. [See Definition 3.8.]

(i) $A = \{x_1, x_2, \dots\} \subseteq \mathbb{N}$ is large if $\sum \frac{1}{x_n} = \infty$.

6.2 Well Distribution

Some sequences in $[0, 1]$ satisfy a distribution property stronger than "uniformly distributed." To discuss that property we consider some different types of limits. The Cesáro limit of a sequence $(a_n)_{n=1}^{\infty}$ is defined as the limit of averages (provided that limit exists):

$$\text{Cesáro limit of } (a_n) = \lim_{N\to\infty} \frac{1}{N} \sum_{i=1}^{N} a_i.$$

6.4 Definition. The sequence $(a_n)_{n=1}^{\infty}$ has *uniform Cesàro limit* a if: $\quad a = \lim\limits_{N-M\to\infty} \dfrac{1}{N-M} \sum\limits_{n=M}^{N-1} a_n.$

This means:

for any $\varepsilon > 0$ there exists L so that: for any interval $\{M, M+1, \ldots, N-1\}$ with $N - M > L$, one has:

$$\left| \frac{1}{N-M} \sum_{n=M}^{N-1} a_n \ - \ a \right| < \varepsilon.$$

6.5 Exercise. Suppose $(a_n)_{n=1}^{\infty}$ is a sequence of numbers.
(1) If the conventional limit exists, $a = \lim\limits_{n\to\infty} a_n$, prove: The uniform Cesáro limit also exists and equals a.

(2) If the uniform Cesáro limit exists, $a = \lim\limits_{N-M\to\infty} \frac{1}{N-M} \sum\limits_{n=M}^{N-1} a_n$, show that the conventional Cesáro limit $\lim\limits_{N\to\infty} \frac{1}{N} \sum\limits_{n=1}^{N} a_n$ also exists and equals a.

(3) Let (a_n) be the sequence $1, -1, 1, -1, \ldots$. Show that $(a_n)_{n=1}^{\infty}$ does not converge, but its uniform Cesáro limit is 0.

More generally, suppose $a_n = \lambda^n$ where $|\lambda| = 1$ in $\mathbb{C}$. Show: Its uniform Cesáro limit is $\begin{cases} 0 & \text{if } \lambda \neq 1, \\ 1 & \text{if } \lambda = 1. \end{cases}$

[Hint. Look at the proof of 2.12.]

(4) Suppose $(a_n)_{n=1}^{\infty}$ is the sequence $1, -1, 1, 1, -1, -1, 1, 1, 1, -1, -1, -1, \ldots$. Show that its Cesáro limit exists, but its uniform Cesáro limit does not.

For further examples of sequences that have Cesáro limits but no uniform Cesáro limits, see Exercise 6.12.

The idea of "well distribution" differs from uniform distribution in the same way that a uniform Cesàro limit differs from a Cesàro limit.

6.6 Definition. A sequence $(x_n)_{n=1}^{\infty} \subset [0,1]$ is *well distributed* (w.d.) if for every $0 \leq a < b \leq 1$,

$$\lim_{N-M\to\infty} \frac{\big|\{n \in [M, N-1] : x_n \in (a,b)\}\big|}{N-M} \ = \ b - a.$$

Certainly, every well-distributed sequence is uniformly destributed. Here is an informal comparison of those two properties. A sequence (x_n) in $[0,1]$ is uniformly distributed if whenever N is large, the proportion of terms $x_1, x_2, \ldots, x_N$ that fall within (a,b) is roughly $b-a$.
The sequence (x_n) is well distributed if whenever $N-M$ is large, the proportion of terms $x_M, x_{M+1}, \ldots, x_{N-1}$ that fall within (a,b) is roughly $b-a$.

Many of the tools that we used to study uniform distribution have analogues for well distribution. Recall that a sequence (x_n) is uniformly distributed mod 1 if and only if for every $f \in C[0,1]$:

$$\frac{1}{N} \sum_{n=1}^{N} f(x_n) \quad \xrightarrow[N\to\infty]{} \quad \int_0^1 f \ dx. \tag{$\dagger$}$$

That criterion has an analogue for well distribution: (x_n) is w.d. (mod 1) if and only if for every $f \in C[0,1]$:

$$\frac{1}{N-M} \sum_{n=M}^{N-1} f(x_n) \quad \xrightarrow[N-M\to\infty]{} \quad \int_0^1 f \ dx. \tag{$\ddagger$}$$

6.7 Exercise. (1) Prove that both criteria ($\dagger$) and ($\ddagger$) above remain true if $C[0,1]$ is replaced by $R[0,1]$, the space of Riemann integrable functions.

(2) Prove that both criteria (†) and (‡) above remain true if $C[0,1]$ is replaced by the collection of all indicator functions $1_{(a,b)}$ for sub-intervals (a,b) of $[0,1]$.

(3) Those criteria (†) and (‡) fail to hold true if f is allowed to be an arbitrary Lebesgue integrable function. [Hint. Let f be the indicator function for $\{x_n\}$.]

6.8 Example. If α is irrational, then $(n\alpha \mod 1)$ is well distributed.

For this argument we can modify the proof in 2.12 using Weyl's criterion, averaging over the interval $[M, N-1]$ rather than $[1, N]$.

6.9 Example. If α is irrational, then $(n^2\alpha \mod 1)$ is also w.d.

For this argument we can modify the ideas in Exercise 4.2. The key step is provided by the following extension of van der Corput's trick.

6.10 Theorem (van der Corput for well distribution)**.**
If $(x_{n+h} - x_n)_{n\in\mathbb{N}}$ is w.d. mod 1 for every $h \in \mathbb{N}$, then $(x_n)_{n\in\mathbb{N}}$ is w.d. mod 1.

As usual, the proof is omitted. Details appear in [8].

The next four exercises illustrate the distinction between u.d. and w.d.

6.11 Exercise. Earlier, in Exercise 3.5, we noted that x is normal (in base 2) if and only if $(2^n x \mod 1)$ is u.d. in $[0,1]$. In contrast, for any x that is normal base 2, show that the sequence $(2^n x \mod 1)$ is *not* well distributed in $[0,1]$. This says that there is no good notion of a number being "uniformly normal."

6.12 Exercise. If $0 < c < 1$, then $(n^c \mod 1)$ is u.d. as seen in (4.7). Show that this sequence is not w.d. in $[0,1]$.

More generally, if $(x_n)_{n\in\mathbb{N}}$ is a sequence in $[0,1]$ such that x_n increases to infinity while $x_{n+1} - x_n \to 0$ and $n(x_{n+1} - x_n) \to \infty$, then (x_n) is u.d. but not w.d. See [27] for details.

6.13 Exercise. $(n^{3/2} \mod 1)$ is u.d. but not w.d. How does this generalize?

6.14 Exercise. If $X = (x_n)_{n=1}^{\infty}$ is a dense sequence in $[0,1]$, can it be rearranged (by permuting the indices) to produce a well distributed sequence?
[Compare Theorem 2.15.]

Remark. A *typical* sequence is u.d. mod 1 but is not w.d. mod 1. To define "typical" we need a notion of measure zero on the space of all sequences. This is done using the *product measure* on $[0,1]^{\mathbb{N}}$. For details see [27] Chapter 3 §2.

7 Topological Dynamical Systems

7.1 Definition. A *topological dynamical system* is a pair (X, T), where $T : X \to X$ is a (bijective) self-homeomorphism of the compact metric space X. (In some contexts we require T to be only a continuous map.)

Here are some examples. Recall that $\mathbb{T}$ is the 1-dimensional torus (i.e. a circle) obtained from the interval $[0, 1]$ by gluing together the endpoints 0 and 1. The metric on $\mathbb{T}$ is usually taken as the arclength between points on the unit circle.

The 2-dimensional torus $\mathbb{T}^2$ is the Cartesian product of two circles: $\mathbb{T}^2 = \mathbb{T} \times \mathbb{T}$. This space can also be viewed as the unit square with opposite edges glued together appropriately.

(1) $X = \mathbb{T}$ and $T_\alpha : X \to X$ defined by $T_\alpha(x) = x + \alpha$.

(2) $X = [0, 1]$ and $T : X \to X$ given by $T(x) = x^{17}$.

(3) $X = \mathbb{T}^2$ and $T : X \to X$ given by $T(x, y) = (x + \alpha, y + 2x + \alpha)$.

7.2 Definition. A subset $Y \subseteq X$ is *T-invariant* if $T(Y) \subseteq Y$.
A *subsystem* of (X, T) is a T-invariant compact subspace of X.

One of the themes in Topological Dynamics is the study of the behavior of orbits of points. If $x_0 \in X$, its *orbit* is the sequence $O(x_0) = (T^n x_0)_{n \geq 0}$ (sometimes we allow $n \in \mathbb{Z}$).

7.3 Exercise. If $Y \subseteq X$ is a T-invariant subset of (X, T), show that its closure $\overline{Y}$ is a subsystem. Since each orbit in X is T-invariant, the closure of an orbit is a subsystem.

7.4 Definition. (X, T) is *minimal* if every orbit is dense.
Then a system is minimal if and only if it has no non-trivial subsystem.

7.5 Exercise. Prove the equivalence stated in Definition 7.4.

7.6 Exercise. Prove: Every topological dynamical system has a minimal subsystem. [Hint. Use Zorn.]

7.7 Exercise. Prove the following:
(a) The dynamical system in example (1) above is minimal if and only if α is irrational.
(b) The system in (2) is not minimal because $Y = \{0\}$ and $Y = \{1\}$ are subsystems of X. In fact, that system has uncountably many subsystems.
(c) If α is irrational then the system in (3) is minimal.

Part (c) in that exercise is non-trivial. For a proof see, for example, Furstenberg's book [20]. Assuming that system is minimal, we derive some interesting consequences. For that system $(\mathbb{T}^2, T)$ in (3), the orbit of $(0, 0)$ is:

$$(0, 0) \to (\alpha, \alpha) \to (2\alpha, 4\alpha) \to \cdots \to (n\alpha, n^2\alpha) \to \ldots$$

Minimality implies that orbit is dense in the torus $\mathbb{T}^2$. Therefore $(n^2\alpha \mod 1)$ is dense in $[0, 1]$.

This idea can be generalized to show that $(n^3\alpha \mod 1)$ is dense in $[0, 1]$. Consider the system $X = \mathbb{T}^3$ and $T : X \to X$ given by $T(x, y, z) = (x + \alpha, y + 2x + \alpha, z + 3x + 3y + \alpha)$. A similar approach shows that for any positive integer k and irrational number α, $(n^k\alpha \mod 1)$ is dense in $[0, 1]$. (Compare (4.2) above.)

In working with dense orbits, it is natural to ask whether that orbit is uniformly dense. If an orbit $(T^n(x))$ is u.d., then there is a *unique invariant measure* on X, the transformation T is automatically ergodic, and the orbit of every point is *well distributed* in X as defined in (6.6). These more advanced concepts of "uniquely ergodic" transformations are discussed in Furstenberg's book [20] in Chapter 3 §2.

7.1 Recurrence in Topological Dynamics

7.8 Definition. For a dynamical system (X, T), a point $x_0 \in X$ is *recurrent* if for every $\varepsilon > 0$, there exists a positive integer N such that $d(x_0, T^N x_0) < \varepsilon$.

In a minimal system (X, T), every orbit is dense so every point is recurrent.

7.9 Lemma. Every dynamical system (X, T) has a recurrent point.

Proof #1. (X, T) has a minimal subsystem (see Exercise 7.6). Every point in that subsystem is recurrent.

Proof #2. Let p be an idempotent ultrafilter as in (5.13). For $x \in X$ let $y = \underset{n\to\infty}{p\text{-lim}}\, T^n x$. Then:

$$\underset{n\to\infty}{p\text{-lim}}\, T^n y = \underset{n\to\infty}{p\text{-lim}}\, T^n \big(\underset{m\to\infty}{p\text{-lim}}\, T^m x \big) = \underset{n\to\infty}{p\text{-lim}} (\underset{m\to\infty}{p\text{-lim}}\, T^{n+m} x) = \underset{n\to\infty}{p\text{-lim}}\, T^n x = y.$$

Here we applied Proposition 5.15. Check that $y = \underset{n\to\infty}{p\text{-lim}}\, T^n y$ implies y is recurrent. □

7.10 Exercise. (1) For the system $(\mathbb{T}, T)$ where $T_\alpha(x) = x + \alpha$, show that every point is recurrent. (Does it matter whether α is irrational?)
(2) For the system $(\mathbb{T}^2, T_{\alpha\beta})$ with $T_{\alpha\beta}(x, y) = (x + \alpha, y + \beta)$, show that every point is recurrent.

7.11 Exercise. If T is an isometry on a compact metric space X, prove that T is surjective.
Find an example showing that this fails for non-compact X.

7.12 Exercise. For a system (X, T) where T is an isometry, show that every point of X is recurrent.

Isometries yield a special class of systems in which every point is recurrent. We now introduce a more general class of systems with this property.

7.13 Definition. A map (not necessarily continuous) T from a metric space X to itself is *distal* if for any $x, y \in X$:

$$\inf_{n\in\mathbb{N}} d(T^n x, T^n y) = 0 \quad \text{implies} \quad x = y.$$

A dynamical system (X, T) is called distal if T is a distal map.

Note that every isometry is distal.

7.14 Theorem. In a distal system, every point is recurrent.

Proof. As in the second proof of Lemma 7.9, let p be an idempotent ultrafilter. For $x \in X$, let $y = \underset{n\to\infty}{p\text{-lim}}\, T^n x$. Then $\underset{n\to\infty}{p\text{-lim}}\, T^n y = \underset{n\to\infty}{p\text{-lim}}\, T^n x = y$. Since T is distal we deduce that $x = y$, and x is recurrent. □

7.15 Exercise. Suppose (X, T) is a dynamical system for which we do not assume T is surjective. If T distal, show that T is surjective.

7.16 Exercise. Consider the system $(\mathbb{T}^2, T)$, where $T(x, y) = (x + \alpha, y + 2x + \alpha)$. As mentioned in (7.7)(c), this system is known to be minimal. Show that it is distal.
[Hint. Here we use the product metric on $\mathbb{T}^2$.]

7.17 Exercise. For systems (X_j, T_j), define the Cartesian product $(X_1, T_1) \times (X_2, T_2) = (X_1 \times X_2, T_1 \times T_2)$ and check that it is a dynamical system.
(1) If X is non-trivial, show that $X \times X$ is not minimal. [Consider $\Delta = \{(x, x) : x \in X\}$.]
(2) If every point is recurrent in (X_j, T_j) for each j, does the same property hold for $(X_1, T_1) \times (X_2, T_2)$?
(3) For which $\alpha, \beta \in \mathbb{R}$ is $(\mathbb{T}^2, T_{\alpha,\beta}) = (\mathbb{T}, T_\alpha) \times (\mathbb{T}, T_\beta)$ a minimal system? Here $T_\alpha(x) = x + \alpha$.

8 More on Topological Dynamics

8.1 Symbolic Space

Historically, Symbolic Dynamics was among the first dynamical systems. Let us consider the symbols $0, 1, \ldots, r-1$ as letters in an alphabet of size r. Symbolic Space is the set of all infinite sequences (words) written in this alphabet. That is, Symbolic Space over $\{0, 1, \ldots, r-1\}$ is the set

$$\Omega_r = \{0, 1, \ldots, r-1\}^{\mathbb{N}}.$$

We often write $x \in \Omega_r$ as an infinite string $x = x_1 x_2 x_3 \cdots$, where each x_r is a symbol in $\{0, \ldots, r-1\}$.

It's also useful to consider finite words in that alphabet. A finite word z is a string of a finite number of symbols: $z = z_1 z_2 \cdots z_n$. Its *length* is the number of symbols in the string (the number of letters in the word). We say that z is a *subword* of a word x if the n symbols comprising z appear as some n consecutive symbols in x. That is, there exists K such that $x_{K+1} = z_1,\ x_{K+2} = z_2,\ \ldots$, and $x_{K+n} = z_n$.

For $x \in \Omega_r$ and $N \in \mathbb{N}$, let $x(N)$ be the initial word of length N in x. That is, $x(N) = x_1 x_2 \cdots x_N$ is the subword of length N that starts off the infinite word x.

Define function d on $\Omega_r \times \Omega_r$ by $d(x, y) := \displaystyle\sum_{n=1}^{\infty} \frac{|x_n - y_n|}{r^n}$.

8.1 Exercise. (a) Show that d is a metric on Ω_r, and $d(x, y) \leq 1$ for every $x, y \in \Omega_r$.
(b) If $x, y \in \Omega_r$, show: $d(x, y) < r^{-N} \iff x(N) = y(N)$.
That is, two words in Ω_r are $\dfrac{1}{r^N}$-close when their first N symbols match.
(c) The space (Ω_r, d) is a compact metric space.

The analogous space Θ_r of bilateral sequences is often considered as well:

$$\Theta_r = \{0, 1, \ldots, r-1\}^{\mathbb{Z}}.$$

The *shift map* $\sigma : \Omega_r \to \Omega_r$ is defined by $\sigma(x) = y$ where $y_n = x_{n+1}$ for every $n \geq 1$. The analogous map is defined similarly on Θ_r. Note that σ is not invertible as a map on Ω_r, but it is invertible as a map on Θ_r.

8.2 Exercise. (1) Show that σ is a continuous map on the compact metric space Ω_r. Consequently, (Ω_r, σ) is a topological dynamical system.
(2) Formulate and prove similar results for Θ_r in place of Ω_r.

Which points in (Ω_r, σ) have a dense orbits? If $x \in \Omega_r$ recall that its orbit is $O(x) = (\sigma^n x)_{n=0}^{\infty}$.

8.3 Theorem. $O(x)$ is dense in (Ω_r, σ) if and only if every finite word appears as a subword of x. In this lecture, we will refer to such x as *topologically normal*. (This is weaker than the version of "normal" mentioned in (3.5).)

Proof. Suppose x is topologically normal. Given $y \in \Omega_r$ and $\varepsilon > 0$, we want to show that some $\sigma^s x$ is ε-close to y. Choose N such that $2^{-N} < \varepsilon$. By hypothesis the finite word $y(N)$ is a subword of x, say starting at some position $s + 1$. Then $\sigma^s x$ begins with that word $y(N)$, and $d(\sigma^s x, y) \leq 2^{-N} < \varepsilon$.

For the converse, suppose $N > 0$. Since $O(x)$ is dense, for any $y \in \Omega_r$ there exists some s such that $d(\sigma^s x, y) < 2^{-N}$. By Exercise 8.1 we know that $\sigma^s x(N) = y(N)$. This says that $y(N)$ occurs as the subword of x starting at position $s + 1$. Since y was arbitrary, we have the desired result. □

8.4 Exercise. If a sequence is normal base 2 (as defined in (3.1)), then it is topologically normal in Ω_2. Prove: Uncountably many elements of Ω_2 are topologically normal but are not normal base 2.

8.5 Exercise. For $x \in \Omega_r$, generalize the proof above to show: $y \in O(x)$ if and only if any finite subword of y is also a subword of x.
It is clear that $\sigma O(x) \subseteq O(x)$. When does equality hold there?

Theorem 8.3 gives a criterion for recurrence of points in (Ω_r, σ), namely:

x is recurrent in $\Omega_r \iff$ Every finite initial word in x appears infinitely many times in x.

We would like to know when the subsystem $\overline{O(x)}$ is minimal. (That's the closure of the orbit of x.) Certainly the whole space (Ω_r, σ) itself is not minimal. For example, the word z consisting entirely of zeros yields a one-element subsystem $\{z\}$. The next exercise provides a criterion for minimality.

8.6 Exercise. Let x be a sequence in Ω_r such that every finite subword w of x appears syndetically. That is, the indices of the first letters of all the occurrences of w in x form a syndetic set (as defined in §11 below). Then $\overline{O(x)}$ is minimal.

8.7 Exercise (Challenging)**.** For $\alpha \in \mathbb{R}$ define $x \in \Omega_2$ by $x(n) = \lfloor n\alpha \rfloor \pmod 2$. Show that that the dynamical system $(\overline{O(x)}, \sigma)$ is minimal.

8.8 Exercise. By considering different values of α in the previous exercise, show that Ω_2 has at least 2 minimal subsystems that are not isomorphic. [Isomorphism is defined in the next section.]

Many natural questions arise in this study of dynamical systems. Here are a few examples.

Are there uncountable many minimal subsystems of (Ω_r, σ)?

What is the probability that a randomly selected $x \in \Omega_r$ is topologically normal?

How can we define sets of measure 0 in symbolic space?

To answer this last question, note that we have a metric so it makes sense to use ε-balls. We can try to mimic the definition of sets of measure 0 in $[0, 1]$ by covering a subset A of Ω_r with an "arbitrarily small amount" of ε-balls. However, to make this precise we need some idea of the volume of a ball.

For a basic idea about this issue, consider the case $r = 2$ and define *cylinders* in Ω_2 as follows. For a finite word w (a list of zeros and ones), let the *cylinder* C_w be the set of all $x \in \Omega_2$ that begin with w. For instance C_{01} is the set of all infinite words that start with 01. There are 2^m words w of length m, and Ω_2 is the disjoint union of those 2^m cylinders C_w. We define the measure of each of those cylinders C_w to be $1/2^m$. Extending this idea, for integer n let the cylinder $C_{n,w}$ be the set of all elements of Ω_2 that contain the word w starting position n. Then $C_w = C_{1,w}$. For $n \in \mathbb{N}$, define the measure of $C_{n,w}$ to be equal to the measure of C_w. This defines a measure μ on all cylinders in Ω_2. Define a subset A of Ω_2 to have measure 0, if for any $\varepsilon > 0$, there exists a countable covering of A by a set of cylinders whose total measure is $< \varepsilon$.

8.2 Isomorphic Topological Dynamical Systems

Topological dynamical systems (X, T) and (Y, S) are "isomorphic" if the topological spaces X, Y are homeomorphic, and the transformations T, S correspond to each other. We need to write down a more precise formulation.

Recall the following definition of homeomophism. A map $\varphi : X \to Y$ of topological spaces is a *homeomorphism* if it is bijective and both φ and φ^{-1} are continuous.

8.9 Exercise. Find an example of a bijective continuous map $\varphi : X \to Y$, such that φ^{-1} is not continuous. Explain why such examples cannot exist when X and Y are compact.

8.10 Definition. A *homomorphism* $\varphi : (X, T) \to (Y, S)$ of topological dynamical systems is a continuous map $\varphi : X \to Y$ such that $\varphi \circ T = S \circ \varphi$. This provides a commutative diagram:

$$\begin{array}{ccc} X & \xrightarrow{T} & X \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ Y & \xrightarrow{S} & Y \end{array}$$

That map φ is an *isomorphism* if φ is a homeomorphism. That is, $\varphi : X \to Y$ is a homeomorphism of topological spaces and φ respects the actions of T and S.
We write $(X, T) \cong (Y, S)$ to mean that there is an isomorphism between them.

Consider the system $(\mathbb{T}, S)$ where $S(x) = 2x \mod 1$. It is natural to attempt to identify this with the system (Ω_2, σ), because multiplication by 2 in $\mathbb{T}$ corresponds to a shift of the binary digits. However, $(\Omega_2, \sigma) \ncong (\mathbb{T}, S)$, since the topological spaces $\mathbb{T}$ and Ω_2 are not homeomorphic. In fact, $\mathbb{T}$ is connected but Ω_2 is not. (Check that $\Omega_2 = C_0 \cup C_1$ is a disjoint union of two closed cylinders.)

8.11 Exercise. Define $T_\alpha(x) = x + \alpha$ on $\mathbb{T}$. For which α, β are the systems $(\mathbb{T}, T_\alpha)$ and $(\mathbb{T}, T_\beta)$ isomorphic?

8.12 Exercise. (1) Find points $x, y \in \Omega_2$ whose orbit-closures $\overline{O(x)}$ and $\overline{O(y)}$ have different cardinalities.
(2) Find x, y such that $\overline{O(x)} \neq \overline{O(y)}$ but they are isomorphic dynamical systems: $(\overline{O(x)}, \sigma) \cong (\overline{O(y)}, \sigma)$.

8.3 Aside: Poncelet's Porism

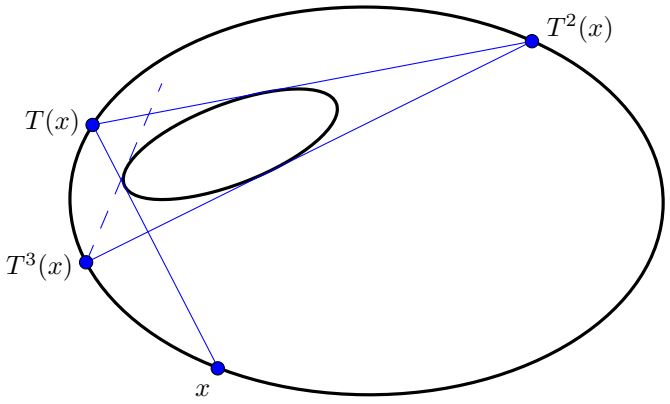
Jean-Victor Poncelet discovered his celebrated porism during 1812-1814 while he was a prisoner of war in Russia. He published it in his 1822 book [33].

Suppose an ellipse E and another ellipse E' inside it are given. For a point x on E, two lines through x are tangent to E'. Choose ℓ to be (say) the left one, and let Tx be the intersection of ℓ with E. This defines a transformation T on the ellipse E.

8.13 Theorem (Poncelet)**.** For the two ellipses E, E' as above, if the transformation T is repeated, then one of the following possibilities occurs:

(1): $T^n x = x$ for some $x \in E$ and some $n > 0$. In this case, $T^n y = y$ for every y on E.

(2): For some $x \in E$, none of the $T^n x$ equals x. In this case, for every y on E, the orbit $\{y, Ty, T^2 y, \dots\}$ is a dense subset of E.



This Theorem was popularized by Jakob Steiner, and many mathematicians have found proofs using a variety of techniques.

It is surprising to realize that Poncelet's transformation T on the ellipse E is closely related to a standard rotation of the circle $\mathbb{T}$. For $\alpha \in \mathbb{R}$, let $\rho_\alpha : \mathbb{T} \to \mathbb{T}$ be the rotation given by $x \mapsto x + \alpha$. One can show that the Poncelet Theorem can be restated to say:

There exists a homeomorphism $\varphi : E \to \mathbb{T}$ and a number α such that the diagram $\begin{array}{ccc} E & \xrightarrow{T} & E \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\varphi} \\ \mathbb{T} & \xrightarrow{\rho_\alpha} & \mathbb{T} \end{array}$ commutes.

Such a homeomorphism φ satisfying $\rho_\alpha \circ \varphi = \varphi \circ T$ is called a **topological conjugacy**.

Given the existence of such φ, Poncelet's Theorem reduces to an examination of iterations ρ_α on $\mathbb{T}$. If α is rational, the orbit of every point is periodic (all with the same period). If α is irrational, then the orbit of any point is dense in $\mathbb{T}$.

Of course it takes some work to prove that that Poncelet's T is conjugate to a rotation of the circle $\mathbb{T}$. For further information see [26]. Poncelet's porism and its relationships to other areas of mathematics continue to be of interest, as seen by the more recent book [17] and articles [14], [23].

9 Measures and Normal Numbers

9.1 Measures

An interval $[a, b]$ has length $b - a$, and it's easy enough to define the "total length" of a finite (or even infinite) union of intervals. We could use open or half-open interals here just as well. Can this notion of length be generalized to a measure on *all* subsets of $\mathbb{R}$? As usual when generalizing an intuitive idea to a precise theory, let's list some properties that we hope such a measure, or "length function," might have. We use $\mu(A)$ (Greek letter mu) for the measure of a subset A. For now we restrict attention to subsets of the unit interval $[0, 1]$.

Here is our wish-list of properties:

(1) Every set has a measure. That is, every subset A is assigned a measure $\mu(A) \geq 0$.

(2) On intervals, the measure equals the length:
If $a \leq b$ then $\mu\big([a, b]\big) = b - a$.

(3) Additivity.
If A, B are disjoint subsets of $[0, 1]$ then $\mu(A \cup B) = \mu(A) + \mu(B)$.
An equivalent, but more general, statement is that μ is "finitely additive":

If $A_1, \ldots, A_n$ are pairwise disjoint subsets of $[0, 1]$, then: $\mu\Big(\bigcup_{j=1}^{n} A_j\Big) = \sum_{j=1}^{n} \mu(A_j)$.

(3)* Countable additivity:

If $A_1, A_2, \ldots,$ are pairwise disjoint subsets of $[0, 1]$, then: $\mu\Big(\bigcup_{j=1}^{\infty} A_j\Big) = \sum_{j=1}^{\infty} \mu(A_j)$.

9.1 Exercise. If μ satisfies (1), (2), and (3), then $\mu(\{a\}) = 0$ for every $a \in [0, 1]$. Therefore, μ assigns the same "measure" to the intervals $[a, b], (a, b], [a, b)$, and (a, b).

It is somewhat surprising to realize that no length function μ can satisfy all these properties! See Exercise 9.11 below.

There are a couple of ways to deal with this impossibility. One is to discard countable additivity, and require only properties (1), (2), and (3). For instance, an ultrafilter on $\Omega = [0, 1]$ satisfies (1), (2), and (3). The study of such "finitely-additive measures" leads to the theory of *invariant means* and is related to the Hausdorff-Banach-Tarski paradox. For example, see [42].

However, we will pursue a different option, retaining countable additivity but allowing some sets to be non-measurable. Then the measure μ is defined on a family of "measurable" subsets of $[0, 1]$. The appropriate sort of family is a σ-algebra.

9.2 Definition. A *σ-algebra* on a set Ω is a non-empty collection $\mathcal{F} \subseteq \mathcal{P}(\Omega)$ that is closed under countable unions and under complements. That is, $\mathcal{F}$ is a nonempty collection of subsets of Ω with the properties:

(a) if $A_j \in \mathcal{F}$ then $\bigcup_{j=1}^{\infty} A_j \in \mathcal{F}$; (b) if $A \in \mathcal{F}$ then $A^c \in \mathcal{F}$.

Next we provide the abstract definition of a measure on a σ-algebra, and the associated measure space.

9.3 Definition. If $\mathcal{F}$ is a σ-algebra on a set Ω, a *measure* is a function $\mu : \mathcal{F} \to [0, \infty]$ satisfying:
$\mu(\varnothing) = 0$ and μ is countably additive: If $A_1, A_2, \cdots \in \mathcal{F}$ are pairwise disjoint then:

$$\mu\Big(\bigcup_{j=1}^{\infty} A_j\Big) = \sum_{j=1}^{\infty} \mu(A_j).$$

In this case we say that $(\Omega, \mathcal{F}, \mu)$ is a *measure space*.

Infinite measures are allowed. For instance, on the real line with a measure extending lengths of intervals, certainly the whole space $\mathbb{R}$ has infinite measure. Most of the measure spaces $(\Omega, \mathcal{F}, \mu)$ we consider are normalized so that $\mu(\Omega) = 1$. With this normalization μ is called a *probability measure*.

9.4 Exercise. (a) If $\mathcal{F}$ is a σ-algebra, show that $\mathcal{F}$ is closed under countable intersections.
(b) Suppose $(\Omega, \mathcal{F}, \mu)$ is a measure space and $A, B \in \mathcal{F}$. Show:
If $A \subseteq B$ then $\mu(A) \leq \mu(B)$.
If $A, B \in \mathcal{F}$, show that $\mu(A \cup B) = \mu(A) + \mu(B) - \mu(A \cap B)$.
How does this generalize to $\mu(A_1 \cup \cdots \cup A_n)$?
(c) Suppose $\mu(A_i \cap A_j) = 0$ whenever $i \neq j$. Does it follow that $\mu\Big(\bigcup_{j=1}^{\infty} A_j\Big) = \sum_{j=1}^{\infty} \mu(A_j)$?

9.5 Exercise. Suppose $\mathcal{F}$ is a σ-algebra.
(1) If $A, B \in \mathcal{F}$ define $A \triangle B$ to be the *symmetric difference* $(A \cup B) \setminus (A \cap B)$. Then $x \in A \triangle B$ if and only if x is in exactly one of A or B. Show that $\mathcal{F}$ becomes a ring, using $\triangle$ as addition and intersection as multiplication. What are zero and one in this ring?

(2) If $\mathcal{F}$ is a finite σ-algebra show that its cardinality $|\mathcal{F}|$ is a power of 2.

Most of the dynamical systems we encounter will have underlying spaces being the unit interval $[0, 1]$, the tori $\mathbb{T}$ and $\mathbb{T}^2$, or a symbolic space such as $\{0, 1\}^{\mathbb{N}}$ and $\{0, 1\}^{\mathbb{Z}}$. Recall that the circle $\mathbb{T}$ is ($\mathbb{R}$ mod 1) and it can also be viewed as the interval $[0, 1]$ with its endpoints glued together. The advantage of using $\mathbb{T}$ rather than $[0, 1]$ is that we avoid worries about shifting sets outside of the interval:
If c is a number and $A \subseteq \mathbb{T}$, then the translation $c + A$ is still inside $\mathbb{T}$.
An "open interval" in the circle $\mathbb{T}$ is either an interval (a, b) in $[0, 1]$, or is "wrapped around": $(a, 1] \cup [0, b)$. Only minor discrepancies between $[0, 1]$ and $\mathbb{T}$ arise from this sort of wrapping. A measure on $[0, 1]$ is essentially the same as a measure on $\mathbb{T}$.

Recall that if Ω is a set then its power set $\mathcal{P}(\Omega)$ is the set of all subsets of Ω.

9.6 Definition. Let $\mathcal{B}(\mathbb{T})$ be the smallest σ-algebra in $\mathcal{P}(\mathbb{T})$ that contains all open intervals (a, b). Similarly define $\mathcal{B}([0, 1])$.
This $\mathcal{B}$ is the *Borel σ-algebra*, and its elements are called *Borel sets* in honor of Émile Borel, a French mathematician and politician.

9.7 Exercise. Show that every closed interval is in $\mathcal{B}(\mathbb{T})$, and every countable subset is in $\mathcal{B}(\mathbb{T})$.
Not every subset of $\mathbb{T}$ is Borel. [Hint: Show that $|\mathcal{B}(\mathbb{T})|$ is smaller then $|\mathcal{P}(\mathbb{T})|$.]

9.8 Proposition. The usual length of intervals in $[0, 1]$ or in $\mathbb{T}$ extends to a unique measure μ on the σ-algebra $\mathcal{B}(\mathbb{T})$ of Borel sets. This measure on $\mathbb{T}$ is translation-invariant. That is, for $A \in \mathcal{B}(\mathbb{T})$ and $c \in \mathbb{R}$: $\mu(c + A) = \mu(A)$.

The proof is left as an exercise. This property holds in $[0, 1]$ as well, provided we work (mod 1). Does the measure μ on $\mathbb{T}$ also satisfy:
$\mu(cA) = c\mu(A)$ for every $A \in \mathcal{B}(\mathbb{T})$ and $c > 0$?

Most sets we deal with are Borel sets so their measures are well-defined.

9.9 Exercise. Cantor-like sets. (1) Recall the Cantor set C as defined in Exercise 1.11. Modify that definition by repeatedly removing "middle intervals" of various lengths. Suppose (a_j) is a sequence with $a_j > 0$ and $\alpha = \sum_{j=1}^{\infty} a_j \leq 1$. At the j^{th} step remove middle intervals with total length a_j. Show that the resulting *Cantor-like* set C' is an uncountable Borel set with $\mu(C') = 1 - \alpha$.

(3) Prove that $C + C = [0, 2]$, for the classical Cantor set C in $[0, 1]$. Does $C - C = [-1, 1]$?
[Hint. Use base 3 expansions to express elements of C.]

(4) Does C contain a Hamel basis? (Such bases were mentioned in (4.14).)

(5) Find a Cantor-like set C' such that all elements of C' are $\mathbb{Q}$-linearly independent. For such C' the difference set $C' - C'$ has empty interior.

In (1.9) above, we defined a notion of sets of "measure zero." That definition does not match our current meaning of $\mu(A) = 0$ because $\mu(A)$ is defined only for Borel sets A. If A is uncountable with $\mu(A) = 0$ there are non-Borel sets A' with $A' \subseteq A$. (Why must such A' exist? See Exercise 9.7.) Let's adjoin such sets A' to the σ-algebra $\mathcal{B}$ and declare them to have measure zero.

9.10 Proposition. Let $\mathscr{Z}$ be the collection of all sets Z in $[0, 1]$ (or $\mathbb{T}$) such that $Z \subseteq A$ for some Borel A with $\mu(A) = 0$. Define $\widehat{\mathcal{B}}$ to be the σ-algebra generated by $\mathcal{B} \cup \mathscr{Z}$. Then μ extends to a measure on $\widehat{\mathcal{B}}$. Moreover, the measure 0 sets defined in (1.9) are the same as sets $A \in \widehat{\mathcal{B}}$ with $\mu(A) = 0$.

Proof. Left as an exercise. It turns out that this family $\widehat{\mathcal{B}}$ coincides with the family of Lebesgue measurable sets. It is interesting to look up the definition of Lebesgue measure and compare these two descriptions.

With only a bit more effort, the Definition 9.6 and Proposition 9.10 can be extended to subsets of $\mathbb{R}$.

A measure space $(X, \mathcal{F}, \mu)$ is called *complete* if every subset of a set of measure zero in $\mathcal{F}$ also lies in $\mathcal{F}$. For example, $(\mathbb{T}, \widehat{\mathcal{B}}, \mu)$ above is complete.

9.11 Proposition. (Due to Giuseppe Vitali, 1905.) Some subsets of $\mathbb{T}$ are not Lebesgue measurable.

The proof shows that the σ-algebra $\mathcal{P}(\mathbb{T})$ of all subsets does not admit a measure that is additively-invariant $\big(\mu(A + c) = \mu(A)\big)$ and satisfies properties (1), (2), (3)* stated at the beginning of this section.

Proof. The idea is that there exist $V \subseteq \mathbb{T}$ and $c_j \in \mathbb{T}$ such that the sets $c_j + V$ are pairwise disjoint and $\mathbb{T} = \bigcup_{j=1}^{\infty}(c_j + V)$. If V is measurable, let $\alpha = \mu(V)$. By (9.8) we know $\mu(c + V) = \alpha$ for every $c \in \mathbb{T}$, and therefore $1 = \mu(\mathbb{T}) = \displaystyle\sum_{j=1}^{\infty} \mu(V + q_j) = \sum_{j=1}^{\infty} \alpha$. Impossible.

To produce such a subset V, consider $Q = (\mathbb{Q} \mod 1)$, a countable subgroup of $\mathbb{T} = (\mathbb{R} \mod 1)$. Then $\mathbb{T}$ is a disjoint union of cosets $v + Q$ for some (uncountable) list of elements v. Let $V \subseteq \mathbb{T}$ be a set that contains exactly one element from each of those cosets. Then every $r \in \mathbb{T}$ is uniquely expressible as $r = v + q$ where $v \in V$ and $q \in Q$. Equivalently, $\mathbb{T}$ is the disjoint union of shifts $V + q$ for $q \in Q$. Since Q is countable, the set V is not measurable, as seen above. □

Note. The Axiom of Choice was used to construct that non-measurable set V. If that axiom is abandoned and the Zermelo-Fraenkel systems of axioms is extended in a different way, then it is possible to build a theory in which *all* subsets of $[0, 1]$ are measurable.

9.2 More on Normal Sequences

Recall that an infinite binary sequence was called normal base 2 if any finite word of zeros and ones appears in the sequence with the appropriate frequency. We sometimes view strings of zeros and ones as coin tossing sequences. Suppose we use an unfair coin for which heads appears with probability p, and tails appears with probability $q = 1 - p$. What would be the corresponding definition of normal? Note that this coin tossing space can be viewed as the symbolic space Ω_2, where heads is 1 and tails is 0.

9.12 Definition. A sequence $\{a_i\}_{i\in\mathbb{N}} \in \Omega_2$ is (p,q)-*normal* if every finite $\{0,1\}$-word $W = (w_i)_{i=1}^k$ consisting of s 1s and $(k-s)$ 0s, satisfies:

$$\lim_{N\to\infty} \frac{\left|\{n \in [1,N] \quad : \quad a_{n+i} = w_i \ \forall\ 1 \le i \le k\}\right|}{N} = p^s q^{k-s}.$$

A notion of measure on Ω_2 was defined at the end of section 8.1. We want a natural way to generalize that notion to the situation when the probabilities p and q are not equal. For a finite word W, let $C_{n,W}$ be the set of all elements of Ω_2 that contain the word W starting at position n. Then we define the measure of $C_{n,W}$ to be $p^s q^{k-s}$ since that is the probability that a randomly selected element from Ω_2 will also be an element of $C_{n,W}$. This does extend to a measure on Ω_2. It is known that with this measure, almost every element of Ω_2 is (p,q)-normal. It is interesting to note that if $(p_1,q_1) \neq (p_2,q_2)$, then a sequence that is (p_1,q_1)-normal cannot be (p_2,q_2)-normal. Moreover, the measure for which the set of (p_1,q_1)-normal elements of Ω_2 a set of measure 1, also makes the set of (p_2,q_2)-normal elements of Ω_2 a set of measure 0.

Here's another example of the surprising behavior of measures. Given $p \in [0,1/2]$, let A_p be the set of $(p,1-p)$-normal sequences in Ω_2. Then: $\bigcup_{p\in[0,1/2]} A_p \subsetneq [0,1]$, even though this is an uncountable union of disjoint sets, and each of those sets has measure 1 under some shift-invariant measure. (Of course we use a different measure for each of the sets A_p).

9.13 Exercise. Find an element of Ω_2 that is not $(p,1-p)$-normal for any $p \in [0,1]$.

10 Introduction to Ergodic Theory

10.1 Measure Preserving Maps and the Ergodic Theorem

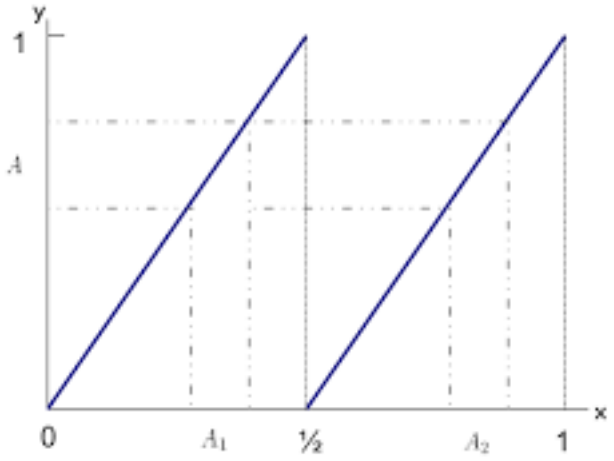
Many interesting maps of $\mathbb{T}$ and $\mathbb{T}^2$ are measure preserving, in the following sense:

10.1 Definition. Suppose $(X, \mathcal{F}, \mu)$ is a measure space with $\mu(X) = 1$, and $T : X \to X$. Then T is called a *measure preserving transformation* if $\mu(A) = \mu(T^{-1}(A))$ for every $A \in \mathcal{F}$.
In this case we say that $(X, \mathcal{F}, \mu, T)$ is a *measure preserving system.*

Note: To check whether a map on $\mathbb{T}$ (or on $[0, 1]$) is measure preserving it suffices to check the property on intervals. More generally:

10.2 Exercise. Suppose the σ-algebra $\mathcal{F}$ is generated by a family of sets $\mathscr{S}$. That means that $\mathcal{F}$ is the smallest σ-algebra containing $\mathscr{S}$. That is, every element of $\mathcal{F}$ can be built from elements of $\mathscr{S}$ by repeated use of the operations of complements and countable unions. (For instance, the open intervals in $\mathbb{T}$ generate the Borel σ-algebra $\mathcal{B}$.) Show that:
A map $T : X \to X$ on $(X, \mathcal{F}, \mu)$ is measure preserving if and only if $\mu(A) = \mu(T^{-1}(A))$ for every $A \in \mathscr{S}$.

Example. The map $S : \mathbb{T} \to \mathbb{T}$ given by $S(x) = 2x \mod 1$ is Lebesgue measure preserving. By (10.2) it suffices to check that S preserves measures of intervals in $[0, 1]$. That property can be seen geometrically using the graph below. For an interval A (on the vertical axis), its pre-image $S^{-1}(A)$ is a union of two intervals each of half the length of A.



Our definition of "measure preserving" uses pre-images $T^{-1}(A)$. Note that this property is quite different from saying that A and its direct image $T(A)$ have the same measure. (Look at the picture above and consider the sets A, A_1, A_2, and $A_1 \cup A_2$.)

10.3 Exercise. Show that the measure preserving transformation $S(x) = 2x \mod 1$ on $\mathbb{T}$ does not preserve measures for direct images $S(A)$.

Any $r \in [0, 1]$ is represented in binary by a sequence of bits (zeros and ones), and the transformation S is just the shift map: $(a_0 a_1 a_2 \cdots) \mapsto (a_1 a_2 a_3 \cdots)$. This S has some similarities with the continued fraction transformation G defined in the next Exercise.

Recall that, in the standard notation for simple continued fractions, $\alpha = [a_0, a_1, a_2, \cdots]$ means:

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\ddots}}}.$$

10.4 Exercise. Define the *Gauss Continued Fraction Transformation* $G : [0,1) \to [0,1)$ as follows:

$$G(0) = 0, \text{ and } G(x) = \tfrac{1}{x} \mod 1 \text{ for } x > 0.$$

(1) Show that $G\big([a_0, a_1, a_2, \cdots]\big) = [a_1, a_2, a_3, \cdots]$. That is, G acts as a shift for continued fraction expansions.

(2) Sketch the graph of $G(x)$ on $[0,1]$. [The graph is a union of many decreasing pieces becoming more crowded near zero.]

(3) Find all $x \in [0,1)$ (in closed form) such that $G(x) = x$.

To extend the analogy between the transformations S and G, recall that a number $r \in [0,1]$ is normal in base 2 when every finite $\{0,1\}$ word appears with the appropriate frequency in the base 2 expansion of r. Can we somehow extend this definition of normality to the continued fraction expansion of a number?

10.5 Exercise. Find a reasonable definition of a "normal" continued fraction. [This is a hard exercise.]

Here's a somewhat more sophisticated point: A transformation that is not measure preserving for Lebesgue measure might be measure preserving for some other measure.

10.6 Exercise. For the Gauss Continued Fraction Transformation $G(x)$, prove:

(1) $G(x)$ does not preserve Lebesgue measure.

(2) $G(x)$ is measure preserving for the measure m on $[0,1]$ defined on intervals by: $m\big((a,b)\big) = \dfrac{1}{\ln(2)} \displaystyle\int_a^b \frac{dx}{1+x}$.

[Hint. Using Exercise 10.2, it suffices to check the measures of $G^{-1}\big([0,a]\big)$.]

10.7 Remark. To say that a property is true *almost everywhere* (often abbreviated a.e.) means that it is false only on a set of measure zero.[1] For instance, if f, f_n, g are functions on $\mathbb{R}$ or on $\mathbb{T}$, then:

$f(x) = g(x)$ almost everywhere, means: $\mu\big(\{c \in \mathbb{R} : f(c) \neq g(c)\}\big) = 0$.

$\lim\limits_{n\to\infty} f_n(x) = g(x)$ almost everywhere, means: $\mu\big(\{c \in \mathbb{R} : \lim\limits_{n\to\infty} f_n(c) \neq g(c)\}\big) = 0$.

f is continuous almost everywhere, means: $\mu\big(\{c : f \text{ is discontinuous at } c\}\big) = 0$.

f is almost everywhere T-invariant means: $\mu\big(\{c : f(Tc) \neq f(c)\}\big) = 0$.

What does it mean to say that sets A, B in $\mathcal{B}$ are equal almost everywhere?

10.8 Definition. Suppose $(X, \mathcal{F}, \mu)$ is a measure space with $\mu(X) = 1$, and $T : X \to X$ is a measure preserving transformation. Then T is *ergodic* if the only sets that are T-invariant almost everywhere are the trivial ones. That is:

the only $A \in \mathcal{F}$ for which $T^{-1}(A) = A$ almost everywhere, satisfy $\mu(A) = 0$ or $\mu(A) = 1$.

[1] The ubiquity of Ross Program alumni might be related to the initials of the Ross Program's founder, Arnold E. Ross. (Remark by D. Shapiro.)

Ergodicity is somewhat analogous to minimality, as defined in (7.4). Suppose $T : X \to X$ is a homeomorphism of a compact metric space X and T is measure preserving for an associated measure on X. Then T is minimal if every point has a dense orbit, while T is ergodic if *almost every* point has a dense orbit. (In fact, for ergodic T, almost every point has a uniformly distributed orbit.)

10.9 Exercise. Suppose $(X, \mathcal{F}, \mu, T)$ is a measure preserving system. Prove: T is ergodic if and only if the only integrable functions that are almost everywhere T-invariant are the constant functions. More precisely, that condition says: if f is an L^1-function on X with $f(Tx) = f(x)$ a.e. then f is constant a.e.

Here we use a standard terminology, saying that f is an L^1-function if f and $|f|$ are integrable, that is, if the integrals $\int_X f\, d\mu$ and $\int_X |f|\, d\mu$ are defined. We write $L^1(X, \mathcal{F}, \mu)$ for the set of L^1 functions on that measure space.

Remark. The map $S(x) = 2x \mod 1$ on $\mathbb{T}$ is ergodic. This is somewhat tricky to prove without more tools. It turns out that this S has the stronger property of "mixing." See Exercise 10.25 below.

The Ergodic Theorem is a statement analogous to our earlier results about uniform distribution. Generalizing an earlier result of von Neumann (see (11.15) below), George David Birkhoff proved his celebrated Pointwise Ergodic Theorem in 1931.

10.10 Theorem (Ergodic Theorem)**.** Suppose $(X, \mathcal{F}, \mu, T)$ is a measure preserving system and $\mu(X) = 1$. If $f \in L^1(X, \mathcal{F}, \mu)$, then the limit $\frac{1}{N}\sum_{n=0}^{N} f\big(T^n x\big)$ exists for almost every $x \in X$.

Moreover, if we define $\widehat{f}(x) = \lim\limits_{N\to\infty} \dfrac{1}{N}\displaystyle\sum_{n=0}^{N} f\big(T^n x\big)$ for almost every $x \in X$, then:

T is ergodic if and only if $\widehat{f}$ is constant almost everywhere, for every $f \in L^1(X, \mathcal{F}, \mu)$.

In that case, $\widehat{f}(x) = \int_X f d\mu$.

10.11 Exercise. In the context of Theorem 10.10, prove that $\widehat{f}$ is almost everywhere T-invariant. That is: $\widehat{f}(Tx) = \widehat{f}(x)$ a.e.

The limit defining $\widehat{f}(x)$ can be viewed as the "time average" of f, while the constant $\int_X f\, d\mu$ can be viewed as the "space average" of f. The Ergodic Theorem is one of the earliest examples of a result stating: the time average equals the space average.

As usual, we omit the proof of this major Theorem. We will include a brief, informal discussion followed by an application.

From a physical point of view, view T as an action on the entirety of some system, such as the movements of a washing machine, constantly moving around the clothes within it. To study the locations of a specific T-shirt[2] in the washing machine throughout time, we can sample its location every second, and average all the samples when we are done. This corresponds to the time average. However, a given T-shirt will eventually visit every location within the washing machine "equally often" in terms of the time it spends there. This says that we expect the locations of the T-shirt over time to be uniformly distributed. The average over all possible locations within the washing machine corresponds to the space average.

The Ergodic Theorem provides a nice proof of a celebrated Theorem of Borel about normal numbers stated as Theorem 3.2 above.

10.12 Theorem. Almost every number in $[0, 1]$ is normal base 2.

[2]This is *not* T applied to shirt. It's a small undershirt, about the size of a point. (Noted by D. Shapiro.)

Proof. For a finite $\{0,1\}$-word $W = (w_1 w_2 \cdots w_n)$, let $a \in [0,1]$ be the number whose binary expansion is the 0-1 sequence W (followed by zeros). That is, $a = \sum w_i 2^{-i}$. Let $b = a + 2^{-n}$. Then $r \in [a,b)$ if and only if the first n binary digits of r equal the word W. Since the transformation $S(x) = 2x \mod 1$ on $\mathbb{T}$ shifts the binary digits, we find:

W is a subword of the first $N+n$ binary digits of $r \iff$ one of $r, Sr, \ldots, S^N r$ lies in $[a,b)$.

Let f be the indicator function of the interval $[a,b)$. Then

The number of times W appears as a subword of the first $N+n$ binary digits of r is:

$$f(r) + f(Sr) + \cdots + f(S^N r).$$

There are $N+1$ subwords of length n in a word of length $N+n$, so the proportion of times W appears equals $\dfrac{1}{N+1}\displaystyle\sum_{j=1}^{N} f(S^j r)$. In the limit, this is exactly $\widehat{f}(r)$.

We are assuming that S is ergodic (see Exercise 10.25 below). The Ergodic Theorem then implies:

$$\widehat{f}(r) = \int_X f \, d\mu = b - a = 2^{-n} \text{ for almost every } r \in [0,1].$$

Then the set $\mathcal{A}_W = \{r \in [0,1] : \widehat{f}(r) = 2^{-n}\}$ is conull (i.e. its complement has measure zero). This is true for every word W of length n. Since there are countably many finite words W, the intersection $\bigcap_W \mathcal{A}_W$ is also conull. That intersection is the set of numbers that are normal base 2.

□

10.13 Exercise. For any integer $m > 1$, show that almost every $r \in [0,1]$ is normal base m.
(Hint. Consider the ergodic transformation $T(x) = mx \mod 1$, and imitate the argument above.)

10.2 Poincaré Recurrence Theorem

10.14 Theorem (Poincaré Recurrence)**.** Suppose $(X, \mathcal{F}, \mu)$ is a measure space (with $\mu(X) = 1$, as usual). For any measure preserving transformation $T : X \to X$ and any $A \in \mathcal{F}$ with $\mu(A) > 0$, there exists integer $n > 0$ such that $\mu(A \cap T^{-n}A) > 0$.

Proof. Consider the sets $A,\ T^{-1}A,\ T^{-2}A,\ T^{-3}A, \ldots$. Since $\mu(X) = 1$ there exist some $i < j$ such that $\mu(T^{-i}A \cap T^{-j}A) > 0$. This equals $\mu(A \cap T^{-(j-i)}A)$ (Why?). Now take $n = j - i$. □

It is somewhat amazing that a statement with such a wonderfully simple proof can lead to so many interesting applications. This theorem can be strengthened in several different directions. The next Exercise contains a useful observation: The integers n can be taken from certain subsets of $\mathbb{N}$. This leads to the study of "sets of recurrence" as defined in (11.7) below.

10.15 Exercise. Suppose $(n_j)_{j=1}^{\infty}$ is an increasing sequence in $\mathbb{N}$, and let $R = \{n_i - n_j : i > j\}$ be the set of differences. Show that in Poincaré's Theorem 10.14, we may choose $n \in R$.

Theorem 10.14 can be strengthened in a different way, as follows.

10.16 Corollary. For $(X, \mathcal{F}, \mu, T)$ and $A \in \mathcal{F}$ with $\mu(A) > 0$, the Poincaré Recurrence Theorem implies:

For almost every $a \in A$, there exists $n > 0$ such that $T^n a \in A$.

That is: Under repeated application of T, a typical point in A eventually revisits A.

Proof. Let A_0 be the set of points of A whose orbits never revisit A. Then A_0 is a measurable set, since $A_0 = A \setminus \left(\bigcup_{n \in \mathbb{Z}^+} (A \cap T^{-n}A)\right)$. For contradiction, assume that $\mu(A_0) > 0$. Poincaré then implies that there

exists $n > 0$ such that $\mu(A_0 \cap T^{-n}A_0) > 0$. If $a_0 \in A_0 \cap T^{-n}A_0$ then $T^n a_0 \in A_0 \subset A$, contradicting the assumption that the orbit of a_0 does not revisit A.

For the converse, assume that for almost every $a \in A$ there exists $n > 0$ such that $T^n a \in A$. That is: $A = \bigcup_{n=1}^{\infty} A \cap T^{-n}A$ almost everywhere. Then

$$0 < \mu(A) = \mu\Big(\bigcup_{n=1}^{\infty} A \cap T^{-n}A \Big) \leq \sum_{n=1}^{\infty} \mu(A \cap T^{-n}A).$$

Then there must exists $n > 0$ such that $0 < \mu(A \cap T^{-n}A)$, as advertised. □

One interesting application of the Poincaré Recurrence Theorem is the following generalization of Kronecker's Theorem, for n numbers rather than one.

10.17 Proposition. Let $(\alpha_i)_{i=1}^n$ be a sequence of irrational numbers and let $\varepsilon > 0$. Then there exists a positive integer m such that $(m\alpha_i \mod 1) \in (0, \varepsilon) \cup (1 - \varepsilon, 1)$ for every $1 \leq i \leq n$.

To see why this is true, let $\mathbb{T}^n$ denote the n-dimensional unit torus, and consider the transformation $T : \mathbb{T}^n \to \mathbb{T}^n$ given by $T\big((x_i)_{i=1}^n\big) = (x_i + \alpha_i)_{i=1}^n$. Check that T is an isometry and hence is measure preserving. Let $A \subset \mathbb{T}^n$ be an arbitrary n-dimensional box of diameter ε. Poincaré Recurrence implies that there exists m such that $\mu(A \cap T^{-m}A) > 0$. Choose $x = (x_1, \ldots, x_n)$ in that intersection. In terms of the Euclidean metric on $\mathbb{T}^n$ we have: $|(m\alpha_1, \ldots, m\alpha_n)| = |T^m x - x| < \varepsilon$. Then $m\alpha_i \in (0, \varepsilon) \cup (1 - \varepsilon, 1)$ for every $1 \leq i \leq n$, as claimed. □

10.3 Mixing

10.18 Definition. Suppose $(X, \mathcal{F}, \mu, T)$ is a measure preserving system. (That is, $(X, \mathcal{F}, \mu)$ is a measure space with $\mu(X) = 1$, and $T : X \to X$ is measure preserving.)
This system if *mixing* if:

$$\text{For any sets } A, B \in \mathcal{F}, \quad \lim_{n\to\infty} \mu(A \cap T^{-n}B) = \mu(A)\mu(B).$$

Every mixing system is ergodic. In fact, one can show that (X, T) is ergodic if and only if it is "mixing on average." That is:

10.19 Theorem. A measure preserving system $(X, \mathcal{F}, \mu, T)$ is ergodic if and only if:

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mu(A \cap T^{-n}B) \;=\; \mu(A)\mu(B), \quad \text{for every } A, B \in \mathcal{F}.$$

To check whether a transformation T is ergodic, it is often easier to check this condition rather than working directly with Definition 10.8. This condition is useful in checking whether a transformation T on $\mathbb{T}$ is ergodic since it suffices to verify it for intervals A, B. In fact, it suffices to check the cases when $A = B$ is an interval.

Proof of Theorem. Let $I_A(x)$ be the indicator function for the set A. Assuming T is ergodic, the Ergodic Theorem implies:

$$\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} I_B(T^n x) = \int I_B(x)dx = \mu(B).$$

Then: $$\int I_A(x) \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} I_B(T^n x)dx = \int I_A(x)\mu(B)dx = \mu(A)\mu(B).$$

Assuming without proof that it's OK to interchange the sum and integral, this equation becomes:

$$\mu(A)\mu(B) = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \int I_A(x) I_B(T^n x) dx =$$
$$= \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \int I_{A\cap T^{-n}(B)}(x) dx = \lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mu(A \cap T^{-n} B).$$

For implication in the other direction, we want to prove T is ergodic, as defined in (10.8). Suppose $A \in \mathcal{F}$ is almost everywhere T-invariant, that is: $A = T^{-1}A$ a.e. From the limit condition in Theorem 10.19 applied to $A = B$, the left side equals $\mu(A)$ while the right side is $\mu(A)^2$. Then $\mu(A) = 0$ or 1, proving ergodicity. $\square$

This interpretation of ergodicity (mixing on average) provides a strengthening of Poincaré Recurrence when T is ergodic. For if we take $A = B$ in (10.19), then:

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

Then there must exist $n > 0$ such that $\mu(A \cap T^{-n} A) \geq \mu^2(A) > 0$, and this verifies Poincaré's conclusion.

10.20 Example. Consider $X = \mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ with measure given by $\mu(A) = \frac{|A|}{5}$. Define $T : X \to X$ by $T(i) = i + 1 \pmod 5$. Then T ergodic, since the only T-invariant subsets are $\varnothing$ and X. However, T is not mixing. For with $A = \{1\}$, note that $\mu(A \cap T^{-n} A) = \begin{cases} \frac{1}{5} & \text{if } n \text{ is a multiple of 5,} \\ 0 & \text{otherwise.} \end{cases}$ This is never very close to $\mu^2(A) = \frac{1}{25}$. It's not hard to verify Theorem 10.19 by checking directly that T is mixing on average.

There are a couple of properties that are between mixing and ergodic.

10.21 Definition. Let $(X, \mathcal{F}, \mu, T)$ be a measure preserving system.

(1) T is *totally ergodic* if T^n is ergodic for every $n \geq 0$.

(2) T is *weakly mixing* if $\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \left|\mu(A \cap T^{-n} B) - \mu(A)\mu(B)\right| = 0$ for every $A, B \in \mathcal{F}$.

It turns out the *typical* (under some advanced notion of "typical") transformation T is weakly mixing.

10.22 Exercise. Show: mixing $\Rightarrow$ weakly mixing $\Rightarrow$ totally ergodic $\Rightarrow$ ergodic.

Remark. These implications are not reversible. The following exercises provide examples for the second and third implications. For examples of systems that are weakly mixing but not mixing, see §4.5 of [31]. (In fact a "typical" transformation is of this type). We omit further details.

10.23 Exercise. The system with $X = \mathbb{Z}/m\mathbb{Z}$ as in Example 10.20 is ergodic but not totally ergodic.

10.24 Exercise. Let $T_\alpha : \mathbb{T} \to \mathbb{T}$ given by $T_\alpha(x) = x + \alpha$. If α is irrational show that T_α is totally ergodic but not weakly mixing.

10.25 Exercise. Show that $S(x) = 2x \mod 1$ is mixing.
[Prove: A transformation is mixing $\iff$ the condition in (10.18) is true on a generating set of $\mathcal{F}$. For this S on $\mathbb{T}$ it suffices to check that condition on intervals of type $[0, c)$.]

11 Varia

11.1 Syndetic Sets

11.1 Definition. A subset $S \subset \mathbb{N}$ is *syndetic* if there exists a positive integer d such that, if the sequence $(s_i)_{i=1}^{\infty}$ is a listing of elements of S in increasing order, then $s_{i+1} - s_i \leq d$ for all i.

In other words, S is syndetic if its gap sizes are bounded. This condition can be viewed as a generalized form of periodicity. Some trivial examples of syndetic sets are $\mathbb{N} - \{1, 2, 3\}$, and $2\mathbb{N}$.

11.2 Exercise. Suppose α is an irrational number.n
(1) Show that $\{\lfloor\alpha\rfloor, \lfloor 2\alpha\rfloor, \lfloor 3\alpha\rfloor, \dots\}$ is syndetic.
(2) For an interval (a, b) in $[0, 1]$, show that $S(a, b) = \{n \mid (n\alpha \mod 1) \in (a, b)\}$ is syndetic.

Proof for (2). Recall that $(n\alpha \mod 1)_{n=1}^{\infty}$ is well distributed, so that $|S(a, b) \cap [N, N + M]| \approx M(b - a)$ for large M.

Alternatively, we can see that $S(a, b)$ is syndetic by recalling that $(n\alpha \mod 1)_{n=1}^{\infty}$ is dense in $[0, 1]$. Let $\varepsilon = \frac{b-a}{3}$, and find positive integers n_1, n_2 and n_3 such that $(n_1\alpha \mod 1) \in (0, \varepsilon)$, $(n_2\alpha \mod 1) \in (1-\varepsilon, 1)$, and $(n_3\alpha \mod 1) \in (a, b)$. For $n \in S(a, b)$, then either $((n + n_1)\alpha \mod 1) \in (a, b)$, or $((n + n_2)\alpha \mod 1) \in (a, b)$ (possibly both). It follows that $S(a, b)$ is syndetic with a gap size bounded by $\max(n_1, n_2)$. □

For any positive integer k, the set

$$S(a, b, k) = \{n \mid (n^k\alpha \mod 1) \in (a, b)\} \text{ is syndetic,}$$

since $(n^k\alpha \mod 1)_{n=1}^{\infty}$ is well distributed. However, for any $c \in (0, 1)$, the set

$$\{n \mid (n^c \mod 1) \in (a, b)\} \text{ is not syndetic provided } (a, b) \neq (0, 1).$$

Indeed, $\lim_{n\to\infty} (n + 1)^c - n^c = 0$, so for any $a > 0$, this sequence spends arbitrarily long amounts of time in either the interval $(0, a)$, or the interval $(1 - a, 1)$.

11.3 Exercise. Let $c > 0$. If $c \notin \mathbb{N}$ show: For any interval $(a, b) \subsetneq (0, 1)$, the set $\{n : (n^c \mod 1) \in (a, b)\}$ is not syndetic. This follows from the fact that (n^c) is not w.d. for $c \in (0, 1)$. See Exercise 6.12.

11.4 Exercise. Suppose $p(x) \in \mathbb{Z}[x]$ is a polynomial and α is an irrational real number. Show that the set $\{n : (p(n)\alpha \mod 1) \in (a, b)\}$ is syndetic.
More generally, suppose $q(x) \in \mathbb{R}[x]$ is a polynomial such that for some $k > 0$, the coefficient of x^k is irrational. Then the set $\{n : (q(n) \mod 1) \in (a, b)\}$ is syndetic.

11.5 Exercise. (1) Prove: Every syndetic subset of $\mathbb{N}$ is AP-rich.
[Hint. Use van der Waerden (3.7). If S is the given set, find $a \in \mathbb{N}$ such that $a + S$ is AP-rich.]

(2) Every syndetic set in $\mathbb{N}$ has positive lower density, as defined in (2.16).

Syndetic sets also occur naturally within ergodic theory. Recall that for an ergodic map T on the measure space $(X, \mathcal{F}, \mu)$ and for any $A \in \mathcal{F}$: $\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \mu(A \cap T^{-n}A) = \mu^2(A)$.

11.6 Remark. In fact, an ergodic map T satisfies a stronger property:

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

This version of the formula is analogous to the strengthening of uniform distribution to well distribution. For details and further extensions, see Corollary 11.17 below.

These ideas can also be used to show that, if T is ergodic, then for any $\varepsilon > 0$ the set $\{n \mid \mu(A \cap T^{-n}A) \in (\mu^2(A) - \varepsilon, \mu^2(A) + \varepsilon)\}$ is syndetic.

11.2 More on Poincaré Recurrence

Examining the proof of Poincaré's Theorem leads to the realization that certain subsets of $\mathbb{N}$ provide a similar conclusion.

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

Poincaré's Theorem says that $R = \mathbb{N}$ is a set of recurrence. Exercise 10.15 shows: If R is the set of all positive differences of an infinite set in $\mathbb{N}$, then R is a set of recurrence.

It follows that for any $n \in \mathbb{N}$, the set $R = n\mathbb{N}$ is a set of recurrence. However, $2\mathbb{N}+1$ is not a set of recurrence, as seen from the example where $X = \{1, 2\}$ with the measure given by cardinality and T that interchanges 1 and 2.

11.8 Exercise. Suppose R is a set of recurrence.
(1) Show that R contains a multiple of every positive integer, and is therefore infinite.
[Hint. Consider $X = \mathbb{Z}/n\mathbb{Z}$ with measure given by cardinality and $Tx = x + 1$.]
(2) If A has zero density, show: $R \setminus A$ is a set of recurrence. (In particular, this holds when A is finite.)
(3) For integer $n > 0$, show that nR is a set of recurrence.
(4) If R_1, R_2 are sets of recurrence, must $R_1 \cap R_2$ also be a set of recurrence?
(5)* For any set of recurrence R, there is a partition $R = R_1 \cup R_2$ where each R_i is a set of recurrence.

11.9 Theorem. The integer squares form a set of recurrence.

This result is sometimes called the "Ergodic Sárközy Theorem," although it was first proved by Furstenberg. In fact, for any positive integer k, the set $R_k = \{n^k\}_{n=1}^{\infty}$ is a set of recurrence.

A closely related result is the "Combinatorial Sárközy Theorem," stated as follows.

11.10 Theorem (Sárközy)**.** For any $E \subset \mathbb{N}$ with $\bar{d}(E) > 0$, there exist distinct $x, y \in E$ such that $x - y$ is a square.

At first sight, it is not at all clear that those two versions of Sárközy's Theorem are related! The connection comes from an early result of Furstenberg, showing that certain sets in $\mathbb{N}$ correspond to measure preserving systems.

11.11 Theorem (**Furstenberg Correspondence Principle).** Let $E \subseteq \mathbb{N}$ be a set with positive upper density: $\bar{d}(E) > 0$. Then there exists a measure preserving system $(X, \mathcal{F}, \mu, T)$ (with $\mu(X) = 1$), and $A \subseteq X$ with $\mu(A) = \bar{d}(E)$, such that for every k and every $n_1, \ldots, n_k \in \mathbb{N}$:

$$\bar{d}\Big(E \cap \bigcap_{i=1}^{k}(E - n_i)\Big) \geq \mu\Big(A \cap \bigcap_{i=1}^{k}(T^{-n_i}A)\Big).$$

For a discussion and proof of this principle, see [1] or [3].

Proof that Ergodic Sárközy implies Combinatorial Sárközy. Given E with positive upper density, apply Furstenberg's Correspondence Principle to obtain the corresponding measure preserving system $(X, \mathcal{F}, \mu, T)$ and subset A. Since $\{n^2\}$ is a set of recurrence by (11.9), there exists a positive integer n such that $\mu(A \cap T^{-n^2}A) > 0$. The inequality in (11.11) then implies: $\bar{d}(E \cap (E - n^2)) \geq \mu(A \cap T^{-n^2}A) > 0$. Consequently there exists $y \in E \cap (E - n^2)$, and we may set $x = y + n^2 \in E$. □

The Ergodic Sárközy Theorem 11.9 will follow using different tools discussed in the next section.

11.3 {Squares} is a Set of Recurrence

In this section we present proofs of the Ergodic Sárközy Theorem 11.9: The squares form a set of recurrence. Before starting that discussion we introduce some of the machinery of Hilbert spaces. We start with some definitions and statements of results without providing all the analytic details.

A *Hilbert space* $\mathscr{H}$ is a complex vector space with an inner product $\langle v, w\rangle$. This is a direct generalization of the finite dimensional space $\mathbb{C}^n$ with inner product given by $\langle v, w\rangle = \sum_{j=1}^{n} v_j \overline{w}_j$. In general, $\langle v, w\rangle$ is a complex number but $||v||^2 = \langle v, v\rangle > 0$ is a positive real number for every nonzero $v \in \mathscr{H}$. This norm $||v||$ satisfies the triangle inequality and induces a metric on $\mathscr{H}$.

An *isometry* on $\mathscr{H}$ is a linear transformation $U : \mathscr{H} \to \mathscr{H}$ satisfying $\langle Uv, Uw\rangle = \langle v, w\rangle$ for every v, w. Check that every isometry is injective. A *unitary operator* on $\mathscr{H}$ is an invertible isometry.

The space $L^2(X, \mu)$ is a particularly important example. For a measure space (X, μ) this space of "square integrable functions" is defined as:

$$L^2(X, \mu) = \{f : X \to \mathbb{C} \ : \ \textstyle\int_X |f|^2 d\mu < \infty\}.$$

If $f, g \in L^2(X, \mu)$ then one can check that $\int_X f\overline{g}\, d\mu$ is defined. We use that value as the inner product:

$$\langle f, g\rangle = \textstyle\int_X f\overline{g}\, d\mu.$$

Strictly speaking, $L^2(X, \mu)$ is the space of all equivalence classes of functions, where f, g are equivalent if $f = g$ almost everywhere. See (10.7). This condition is needed to ensure that $||f|| = 0$ only when $f = 0$. Then $L^2(X, \mu)$ is a Hilbert space.

For sets $A, B \in \mathcal{F}$ note that $\langle 1_A, 1_B\rangle = \int_X 1_A \cdot 1_B\, d\mu = \mu(A \cap B)$.

11.12 Lemma. Let $(X, \mathcal{F}, \mu, T)$ be a measure preserving system. Define $U_T : L^2(X, \mu) \to L^2(X, \mu)$ by: $U_T(f) = f \circ T$. Then U_T is an isometry on $L^2(X, \mu)$.

Proof. We outline several steps, leaving the details as an exercise.

$U_T : L^2(X, \mu) \to L^2(X, \mu)$ is a linear transformation.

$U_T 1_A = 1_{T^{-1}A}$ for every $A \in \mathcal{F}$ and $\langle U_T 1_A, U_T 1_B\rangle = \mu(A \cap B) = \langle 1_A, 1_B\rangle$.

$\langle U_T f, U_T g\rangle = \langle f, g\rangle$ for every $f, g \in L^2(X, \mu)$. [Approximate f, g via 1_A functions.] □

Since our main application of Hilbert spaces is to the space L^2, we use letters f, g to stand for elements of a general Hilbert space $\mathscr{H}$.

On a finite dimensional space, every isometry is invertible. An isometry on a Hilbert space is always injective but might fail to be surjective.

11.13 Exercise. (1) $Tx = (2x \mod 1)$ is a measure preserving on $\mathbb{T}$, so U_T is an isometry on $L^2(\mathbb{T}, \mu)$. Show that U_T is not surjective.
[Hint. Apply U_T to the basis elements $e^{2\pi inx}$ of $L^2(\mathbb{T})$.]
(2) If $(X, \mathcal{F}, \mu, T)$ is a measure preserving system and T is invertible, show that U_T is a unitary operator.

If $W \subseteq \mathscr{H}$ is a subspace, its *orthogonal complement* $W^\perp$ is defined by:

$$f \in W^\perp \text{ if and only if } \langle f, g\rangle = 0 \text{ for every } g \in W.$$

In other words, $W^\perp = \{f \in \mathscr{H} : \langle f, W\rangle = 0\}$. Then $W^\perp$ is a subspace of $\mathscr{H}$ and it is closed (using the

topology coming from the norm). Moreover, $W \cap W^\perp = \{0\}$ and $W \subseteq \overline{W} \subseteq (W^\perp)^\perp$, where the bar denotes the topological closure. After some work with the definitions it follows that:

If W is a subspace, then: $(W^\perp)^\perp = \overline{W}$.

If W is a closed subspace then $W = (W^\perp)^\perp$ and $\mathscr{H} = W \oplus W^\perp$.

For any bounded linear operator A on $\mathscr{H}$ there exists an *adjoint* A^* that is a linear operator satisfying:

$$\langle Af, g\rangle = \langle f, A^*g\rangle \text{ for every } f, g \in \mathscr{H}.$$

We omit the details of defining "bounded," proving that the adjoint exists, verifying that $(A^*)^* = A$, etc.

For a unitary operator U on $\mathscr{H}$ it follows that $U^* = U^{-1}$.

Consider a unitary operator U on the Hilbert space $\mathscr{H}$. Without defining "adjoints" generally, we let $U^* = U^{-1}$ so that

$$\langle Uf, g\rangle = \langle f, U^*g\rangle \text{ for every } f, g \in \mathscr{H}.$$

An element $f \in \mathscr{H}$ is called *invariant* if $Uf = f$, and we define $\mathscr{H}_{inv}$ to be the subspace of invariant vectors:

$$\mathscr{H}_{inv} = \{f \in \mathscr{H} : \ Uf = f\}.$$

This is a closed subspace, and its orthogonal complement is defined as $\mathscr{H}_{erg} = \mathscr{H}_{inv}^\perp$.

11.14 Lemma. $\mathscr{H}_{erg} = span\{f - Uf : \ f \in \mathscr{H}\}$.

Proof. Let W be the right side of the equation in (11.14). By "span" here we mean to allow infinite (convergent) linear combinations. Equivalently, W is the closure of the linear subspace of all vectors $f - Uf$.

Furthermore: $h = 0 \iff \langle h, f\rangle = 0$ for every $f \in \mathscr{H}$. (For $h \neq 0$ in $\mathscr{H}$ implies $||h|| > 0$.)
Then:

$$\begin{aligned} g \in W^\perp &\iff \langle g, f - Uf\rangle = 0 \quad \text{for every } f \in \mathscr{H} \\ &\iff \langle g - U^*g, f\rangle = 0 \ \text{ for every } f \in \mathscr{H} \qquad (\text{using } (U^*)^* = U \text{ here}) \\ &\iff g = U^*g \iff g \in \mathscr{H}_{inv}. \end{aligned}$$

Therefore, $W = \mathscr{H}_{inv}^\perp = \mathscr{H}_{erg}$. □

Now we can prove the seminal Ergodic Theorem of John von Neumann, as proved in [30] in 1932. See [5] for some of the history.

11.15 Theorem (von Neumann)**.** Suppose U is a unitary operator on a Hilbert space $\mathscr{H}$ and $f \in \mathscr{H}$. Then $\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} U^n f$ converges to some Pf in $\mathscr{H}$ (using the metric derived from the norm).
Then $Pf \in \mathscr{H}_{inv}$ and the map $P : f \mapsto Pf$ is the orthogonal projection $\mathscr{H} \to \mathscr{H}_{inv}$.

Proof. There is an orthogonal splitting $\mathscr{H} = \mathscr{H}_{inv} \oplus \mathscr{H}_{erg}$, as above. It suffices to check the limit on each term. If $f \in \mathscr{H}_{inv}$ then $Uf = f$ so that $\frac{1}{N}\sum_{n=1}^{N} U^n f = f$ and the limit is $Pf = f$. If $f \in \mathscr{H}_{erg}$ then by Lemma 11.14, we may assume $f = h - Uh$ for some $h \in \mathscr{H}$. Then $\sum_{n=1}^{N} U^n f = \sum_{n=1}^{N} U^n(h - Uh)$ telescopes, equaling $Uf - U^{n+1}f$ so the limit in question is zero, because of the denominator N. Therefore $f \mapsto Pf$ is the identity on $\mathscr{H}_{inv}$ and is zero on $\mathscr{H}_{erg}$. □

This argument also proves that $\mathscr{H}_{erg} = \{f \in \mathscr{H} : \ \frac{1}{N}\sum_{n=1}^{N} U^n f \to 0\}$.

Von Neumann's Ergodic Theorem extends nicely to a version with *uniform limits* of the types in our discussions of well distribution.

11.16 Corollary. If U is a unitary operator acting on a Hilbert space $\mathscr{H}$, then for any $f \in \mathscr{H}$,

$$\lim_{N-M\to\infty} \frac{1}{N-M} \sum_{n=M}^{N-1} U^n f = Pf,$$

where the convergence is in norm and, as before, Pf is the orthogonal projection of f to $\mathscr{H}_{inv}$.

This uniform version of von Neumann's Theorem 11.15 follows from the same proof, and we omit details. As one consequence, we deduce an inequality related to the property in (11.6).

11.17 Corollary. Every measure preserving system $(X, \mathcal{F}, \mu, T)$ satisfies the inequality:

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

Furthermore: T is ergodic if and only if equality holds there for every $A \in \mathcal{F}$.

Proof. The projection Pf satisfies: $PP = P$ and $\langle Pf, g\rangle = \langle f, Pg\rangle = \langle Pf, Pg\rangle$ for every $f, g \in \mathscr{H}$. We use the operator $U = U_T$ on $\mathscr{H} = L^2(X, \mathcal{F}, \mu)$. Then for $f = 1_A$ we have:

$$\begin{aligned}
&\lim_{N-M\to\infty} \frac{1}{N-M} \sum_{n=M}^{N-1} \mu(A \cap T^n A) \\
&= \lim_{N-M\to\infty} \frac{1}{N-M} \sum_{n=M}^{N-1} \langle U^n f, f\rangle \\
&= \langle Pf, f\rangle \quad \text{by continuity of } h \mapsto \langle h, f\rangle, \\
&= \langle Pf, Pf\rangle.
\end{aligned}$$

By Cauchy-Schwarz, and since $P1 = 1$, that becomes: $\langle Pf, Pf\rangle\langle 1, 1\rangle \geq \big(\langle Pf, 1\rangle\big)^2 = \big(\langle f, 1\rangle\big)^2 = \mu(A)^2$. □

Before getting to sets of recurrence we need to introduce one more analytic tool.

11.18 Definition. A sequence $(a_n)_{n\in\mathbb{Z}}$ in $\mathbb{C}$ is **positive definite** if for every $N \in \mathbb{N}$ and any numbers $\xi_j \in \mathbb{C}$:

$$\sum_{-N\leq m,n\leq N} a_{n-m}\xi_n\overline{\xi}_m \geq 0.$$

For instance, a non-negative constant sequence is positive definite. (Exercise.)

11.19 Lemma. Suppose U is a unitary operator on a Hilbert space $\mathscr{H}$, and $f \in \mathscr{H}$. Then the sequence $a_n = \langle U^n f, f\rangle$ is positive definite.

Proof. Let $N \in \mathbb{N}$. Then

$$\sum_{-N\leq m,n\leq N} \langle U^{n-m} f, f\rangle \xi_n\overline{\xi}_m = \sum_{-N\leq m,n\leq N} \langle U^n f, U^m f\rangle \xi_n\overline{\xi}_m = \Big\langle \sum_{-N\leq n\leq N} U^n f\xi_n, \sum_{-N\leq m\leq N} U^m f\xi_m \Big\rangle \geq 0. \qquad \square$$

Since U is unitary we have a clear definition of a_n for $n < 0$. The ideas still work when U is assumed to be an isometry (not necessarily invertible). In that case, we modify the definition of the sequence as follows: $a_n = \begin{cases} \langle U^n f, f\rangle & \text{if } n \geq 0, \\ \langle (U^*)^{|n|} f, f\rangle & \text{if } n < 0. \end{cases}$ With this modification, most of the results stated here for unitary operators are true more generally for isometries. However, to keep the exposition clearer we restrict attention to unitary operators during this section.

11.20 Corollary. Suppose $(X, \mathcal{F}, \mu, T)$ is a measure preserving system. Then for any $A \in \mathcal{F}$, the sequence $a_n = \mu(A \cap T^n A)$ is positive definite.

Proof. (11.12) implies that $a_n = \mu(A \cap T^n A) = \langle U_T^n 1_A, 1_A\rangle$, and Lemma 11.19 shows that $(a_n)_{n\in\mathbb{Z}}$ is a positive definite sequence. □

11.21 Exercise. Suppose $E \subseteq \mathbb{N}$ and let $a_n = \overline{d}(E \cap (E - n))$. Then $(a_n)_{n\in\mathbb{Z}}$ is positive definite.

We now state a non-trivial result that characterizes positive definite sequences. A version of this theorem was proved in 1911 by Gustav Herglotz [24]. (Herglotz was E. Artin's doctoral adviser). We will accept Herglotz's Theorem as a fact, and use it to help prove (11.9).

11.22 Theorem (Herglotz)**.** A sequence $(a_n)_{n\in\mathbb{Z}} \subset \mathbf{C}$ is positive definite if and only if it is the Fourier transform of a positive measure ν on $\mathbb{T}$. In fact, one can choose ν to be a finite Borel measure, that is, a measure defined on the Borel σ-algebra defined in (9.6).

That is, in order for a sequence $(a_n)_{n\in\mathbb{Z}}$ to be positive definite, there must exist a positive measure ν on $\mathbb{T}$ with the property that (for all $n \in \mathbb{Z}$),

$$a_n = \widehat{\nu}(n) = \int_{\mathbb{T}} e^{2\pi i n t}\, d\nu(t).$$

We use the term "positive measure" here to indicate that $\nu(S) \geq 0$ for every measurable S. This property was part of our definitions, but in more general contexts people often allow measures to have negative values (a "signed measure").

Note: This transform of a measure is sometimes called the Fourier-Stieltjes transform. It generalizes the Fourier transform of a function. The usual Fourier Transform of an integrable function $f(x)$ on $\mathbb{T}$ is: $\widehat{f}(t) = \int_{\mathbb{T}} e^{2\pi i x t} f(x)\, dx$, where dx corresponds to Lebesgue measure on $\mathbb{T}$. Define measure ν associated to f by: $\nu(A) = \int_A f(x)\, dx$. [Exercise. Check that this ν is a measure.] Then the transform $\widehat{\nu}$ above equals

$$\widehat{\nu}(n) = \int_{\mathbb{T}} e^{2\pi i n t}\, d\nu = \int_{\mathbb{T}} e^{2\pi i n t} f(x)\, dx = \widehat{f}(n).$$

We are particularly interested in the sequences arising in (11.20) and hence from (11.19). So suppose U is a unitary operator on Hilbert space $\mathscr{H}$. Then each $f \in \mathscr{H}$ induces a positive definite sequence $a_n = \langle U^n f, f\rangle$, and by Herglotz's Theorem 11.22 we have a corresponding measure ν_f. Then, by the definitions:

$$\langle U^n f, f\rangle = \widehat{\nu}_f(n) = \int_{\mathbb{T}} e^{2\pi i n t} d\nu_f.$$

This measure ν might not be as nice as our familiar examples. There might be a singleton set with positive measure: $\nu\big(\{a\}\big) > 0$. Such "large" points a are called *atoms* for ν. A measure with atoms can be counter-intuitive because this can cause finite sets to be non-negligible in integrals. We will now show that atoms of ν_f are closely related to eigenvalues of U.

Suppose $Uf = \lambda f$ for some scalar λ. Since U is unitary we see that $|\lambda| = 1$ and we may express $\lambda = e^{2\pi it}$ for some $t \in \mathbb{T}$. (As usual, $\mathbb{T}$ is the same as $\mathbb{R} \mod 1$.)

11.23 Proposition. Let U be a unitary operator on Hilbert space $\mathscr{H}$ and $f \in \mathscr{H}$. Let ν_f be the measure associated with the positive definite sequence $a_n = \langle U^n f, f\rangle$. Then for $t \in \mathbb{T}$:

$$t \text{ is an atom for } \nu_f \quad \text{if and only if} \quad \lambda = e^{2\pi it} \text{ is an eigenvalue for } U.$$

Proof. Suppose $Uf = \lambda f$ where $\lambda = e^{2\pi it}$. Then $U^n f = e^{2\pi int} f$ for every n. Therefore

$$\langle f, f\rangle = \frac{1}{N}\sum_{n=0}^{N-1} e^{-2\pi int}\langle U^n f, f\rangle = \frac{1}{N}\sum_{n=0}^{N-1} e^{-2\pi int}\int_{\mathbb{T}} e^{2\pi inx} d\nu_f(x) = \int_{\mathbb{T}} \frac{1}{N}\sum_{n=0}^{N-1} e^{2\pi in(x-t)} d\nu_f(x).$$

This holds true for every N, and in taking the limit recall that:

$$\text{For any } w \in \mathbb{C} \text{ with } |w| = 1, \quad \frac{1}{N}\sum_{n=0}^{N-1} w^n \to \begin{cases} 1 & \text{if } w = 1, \\ 0 & \text{if } w \neq 1. \end{cases}$$

The equations above then imply: $||f||^2 = \nu_f\big(\{t\}\big)$, and t is an atom.

For the converse, suppose $t \in \mathbb{T}$ and define a unitary operator $V : \mathscr{H} \to \mathscr{H}$ by $Vf = e^{-2\pi it} Uf$. Von Neumann's Theorem 11.15 implies that $Pf = \lim_{N\to\infty} \frac{1}{N}\sum_{n=0}^{N-1} V^n f$ is defined, and $VPf = Pf$. Then $UPf = e^{2\pi it} Pf$. If we can show $Pf \neq 0$ then $\lambda = e^{2\pi it}$ is an eigenvalue for U, as hoped.

Compute the inner product

$$\langle \widetilde{f}, f\rangle = \lim_{N\to\infty} \frac{1}{N}\sum_{n=0}^{N-1} e^{-2\pi int}\langle U^n f, f\rangle = \lim_{N\to\infty} \int_{\mathbb{T}} \frac{1}{N}\sum_{n=1}^{N-1} e^{2\pi in(x-t)} d\nu_f = \nu_f\big(\{t\}\big),$$

for similar reasons as before. Therefore, if t is a atom for ν then $\langle \widetilde{f}, f\rangle > 0$ and $\widetilde{f} \neq 0$, as claimed. □

We want to apply these ideas to the positive definite sequence (a_n) where $a_n = \mu(A \cap T^n A)$ for a measure preserving system $(X, \mathcal{F}, \mu, T)$ as in (11.20). The Hilbert space here is $\mathscr{H} = L^2(X, \mu)$ with $U = U_T$. Since the constant function 1_X is an eigenvector (certainly $U(1_X) = 1_X$), we know from (11.23) that 0 is an atom for the measure ν. To avoid this case, let's split $\mathscr{H}$ as: $\mathscr{H} = \mathbb{C} \oplus \mathscr{H}_0$, where $\mathscr{H}_0 = (1)^\perp$ consists of all g with $\int_X g\, d\mu = 0$. Since U is an isometry, the space $\mathscr{H}_0$ is U-invariant.

11.24 Corollary. If $f_0 \in \mathscr{H}_0$ and $b_n = \langle U^n f_0, f_0\rangle$, then (11.19) implies that (b_n) is positive definite, and Herglotz (11.22) yields a measure ν on $\mathbb{T}$. If T is totally ergodic, the atoms of ν are irrational.

Proof. If $t \in \mathbb{T}$ is an atom then $\lambda = e^{2\pi it}$ is an eigenvalue for $U = U_T$, so there exists some nonzero $g \in \mathscr{H}_0$ with $Ug = \lambda g$. If t is rational then $\lambda^n = 1$ for some $n > 0$ and $U^n g = g$. This means that $g(T^n x) = g(x)$ for almost every $x \in X$. If T is totally ergodic as defined in (10.21), then T^n is ergodic and the function g must be constant (see Exercise 10.9). Since $\int_X g\, d\mu = 0$, we find that $g = 0$, contrary to hypothesis. □

Our goal is to use these ideas to gain some insight into the Ergodic Sárközy Theorem 11.9, stating that the squares form a set of recurrence.

Proof of (11.9) in the case T is totally ergodic.
Following Definition 11.7, for a measure preserving system $(X, \mathcal{F}, \mu, T)$ and set $A \in \mathcal{F}$ with $\mu(A) > 0$, we hope to prove:

$$\mu(A \cap T^{-n^2} A) > 0 \text{ for some integer } n > 0.$$

The analysis begins with $\mathscr{H} = L^2(X, \mu)$ and unitary operator $U = U_T$. (We avoid technicalities by making the mild assumption that T is invertible so that U_T is unitary.) Let $f = 1_A$ be the indicator function for the given set A. As noted in the proof of Lemma 11.12:

$$\mu(A \cap T^{-n}A) = \langle 1_A, U^n 1_A \rangle = \int_X f \; U^n f \, d\mu.$$

Since T is invertible and measure preserving this also equals $\mu(A \cap T^n A)$. We may switch n and $-n$ whenever it's convenient.

11.25 Claim. If T is totally ergodic, then: $\quad \dfrac{1}{N} \displaystyle\sum_{n=1}^{N} \mu(A \cap T^{n^2}A) \; \to \; \mu^2(A).$

If this Claim is true, then since $\mu(A) > 0$ there must exist infinitely many n for which $\mu(A \cap T^{n^2}A) > 0$, completing the proof.

To prove the Claim 11.25, split $\mathscr{H} = \mathbb{C} \oplus \mathscr{H}_0$ as above, where $\mathscr{H}_0$ consists of all g with $\int_X g \, d\mu = 0$. Since $\langle 1_A, 1 \rangle = \int_X f \, d\mu = \mu(A)$ we have $f = 1_A = \mu(A) + f_0 \in \mathbb{C} \oplus \mathscr{H}_0$, where $f_0 = 1_A - \mu(A) \in \mathscr{H}_0$. Therefore:

$$\begin{aligned} \mu(A \cap T^n A) &= \int_X 1_A \; U^n 1_A \; d\mu = \\ &= \mu^2(A) + \int_X f_0 \; U^n f_0 \; d\mu. \end{aligned}$$

The Claim will follow if we show that $\quad \dfrac{1}{N} \displaystyle\sum_{n=1}^{N} \int_X f_0 \; U^{n^2} f_0 \; d\mu \; \longrightarrow \; 0.$

That term equals $\frac{1}{N} \sum\limits_{n=1}^{N} a_{n^2}$ where $a_n = \langle U^n f_0, f_0 \rangle = \int_X f_0 \; U^n f_0 \; d\mu$. Since (a_n) is positive definite by (11.19), Herglotz's Theorem 11.22 provides a measure ν on $\mathbb{T}$ such that $a_n = \int_{\mathbb{T}} e^{2\pi i n t} \; d\nu(t)$. Then

$$\frac{1}{N} \sum_{n=1}^{N} \int_X f_0 \; U^{n^2} f_0 \; d\mu = \frac{1}{N} \sum_{n=1}^{N} \int_{\mathbb{T}} e^{2\pi i n^2 x} \; d\nu(x) = \int_{\mathbb{T}} \frac{1}{N} \sum_{n=1}^{N} e^{2\pi i n^2 x} \; d\nu(x).$$

We have seen that sort of inner sum before! If x is irrational we remarked in (4.2) that $(n^2 x \mod 1)_{n=1}^{\infty}$ is uniformly distributed. Weyl's Criterion 2.5 then implies: $\quad \dfrac{1}{N} \displaystyle\sum_{n=1}^{N} e^{2\pi i n^2 x} \longrightarrow 0.$

To complete the proof, we need to verify that we may ignore the rational values of x. This is clear if we know that the set of rationals in $\mathbb{T}$ has measure zero for ν. A countable set has measure zero exactly when it contains no atoms. Since T is totally ergodic, Corollary 11.24 finishes our work. □

Now we outline a different approach to the Ergodic Sárközy Theorem 11.9, using a more geometric argument.

This approach will settle the problem for general measure preserving systems $(X, \mathcal{F}, \mu, T)$. (The previous method yielded the result only for totally ergodic systems.) As before, we make the mild assumption that T is invertible so that $U = U_T$ is a unitary operator on the Hilbert space $\mathscr{H} = L^2(X, \mu)$.

Recall from the proof of von Neumann's Theorem (11.15) that there is an orthogonal splitting $\mathscr{H} = \mathscr{H}_{inv} \oplus \mathscr{H}_{erg}$ where:

$$\mathscr{H}_{inv} = \{f \in \mathscr{H} : \; Uf = f\} \qquad \text{and} \qquad \mathscr{H}_{erg} = \{f \in \mathscr{H} : \; \tfrac{1}{N} \sum_{n=1}^{N} U^n f \to 0\}.$$

Using U^k in place of U yields a corresponding splitting for every $k \geq 1$:

$$\mathscr{H} = \mathscr{H}_{inv}^{(k)} \oplus \mathscr{H}_{erg}^{(k)}.$$

Note that $\mathscr{H}_{inv}^{(i)} \subseteq \mathscr{H}_{inv}^{(j)}$ whenever $i \mid j$. This shows that the union of all $\mathscr{H}_{inv}^{k}$ is a linear subspace of $\mathscr{H}$, but it might not be closed. We define:

$$\mathscr{H}_{rat} = \overline{\bigcup_k \mathscr{H}_{inv}^{(k)}}, \quad \text{the closure of that linear subspace.}$$

$$\mathscr{H}_{tot.erg} = \bigcap_k \mathscr{H}_{erg}^{(k)}.$$

11.26 Lemma. Using notations above, $\mathscr{H} = \mathscr{H}_{rat} \oplus \mathscr{H}_{tot.erg}$ is an orthogonal splitting, and:

$$\mathscr{H}_{rat} = span\{f \in \mathscr{H} : \, U^k f = f \text{ for some } k > 0\}$$
$$= span\{f \in \mathscr{H} : \, Uf = \lambda f \text{ for some root of unity } \lambda\}.$$

$$\mathscr{H}_{tot.erg} = \{f : \, ||\tfrac{1}{N} \sum_{n=1}^{N} U^{kn} f|| \to 0 \text{ for every } k\}.$$

As before the "span" includes infinite (convergent) linear combinations. If $K \subseteq \mathscr{H}$ is subset, then $span(K)$ is the closure of the linear subspace generated by K.

The proof of this Lemma is left as an exercise.

We want to prove Ergodic Sárközy Theorem 11.9, stating that the squares form a set of recurrence. This means that for any measure preserving $(X, \mathcal{F}, \mu, T)$ and any set $A \in \mathcal{F}$ with $\mu(A) > 0$, we hope to prove that $\mu(A \cap T^{-n^2} A) > 0$ for some positive integer n.

As in the previous discussion, this can be restated in Hilbert space terms since $\mu(A \cap T^{-n} A) = \langle U^n 1_A, 1_A \rangle$. So we will prove: $\quad \langle U^{n^2} 1_A, \ 1_A \rangle > 0$ for some integer $n > 0$.

That inequality will follow for infinitely many n, once we prove the following:

$$\text{There exists } M > 0 \text{ such that } \Big\langle \frac{1}{N} \sum_{n=1}^{N} U^{(Mn)^2} 1_A \ , \ 1_A \Big\rangle \text{ has a positive limit as } N \to \infty.$$

Our strategy is to express $1_A = f_1 + f_2$ using the splitting $\mathscr{H} = \mathscr{H}_{rat} \oplus \mathscr{H}_{tot.erg}$. Since those subspaces of $\mathscr{H}$ are orthogonal and U-invariant, we have $\langle U^n(f_1 + f_2), f_1 + f_2 \rangle = \langle U^n f_1, f_1 \rangle + \langle U^n f_2, f_2 \rangle$. Therefore we may analyze those two components separately.

For the totally ergodic piece, we note that van der Corput's Difference Theorem 4.1 extends to Hilbert spaces as follows.

11.27 Proposition. If (x_n) is a bounded sequence in $\mathscr{H}$ and if $\lim_{N\to\infty} \frac{1}{N} \sum_{n=1}^{N} \langle x_{n+h}, x_n \rangle = 0$ for every $h \in \mathbb{N}$, then $\lim_{N\to\infty} \big|\big| \frac{1}{N} \sum_{n=1}^{N} x_n \big|\big| = 0$.

A proof is presented in the survey article [3] p. 15.

11.28 Lemma. If $f \in \mathscr{H}_{tot.erg}$, then: $\frac{1}{N} \sum_{n=1}^{N} U^{n^2} f \longrightarrow 0$.

Proof. For $x_n = U^{n^2} f$ we have $\langle x_{n+h}, x_n \rangle = \langle U^{n^2+2nh+h^2} f, \ U^{n^2} f \rangle = \langle U^{(2h)n} f, U^{-h^2} f \rangle$. Since $f \in \mathscr{H}_{tot.erg}$ we know that $||\frac{1}{N} \sum_{n=1}^{N} U^{kn} f|| \to 0$ for every k. Therefore $\frac{1}{N} \sum_{n=1}^{N} \langle U^{kn} f, g \rangle \longrightarrow 0$ for every g (by Cauchy-

Schwarz). Consequently, for every $h \in \mathbb{N}$, $\lim_{N\to\infty} \frac{1}{N}\sum_{n=1}^{N}\langle x_{n+h}, x_n\rangle = \lim_{N\to\infty}\left\langle \frac{1}{N}\sum_{n=1}^{N} U^{(2h)n} f,\ U^{-h^2} f\right\rangle = 0$. Then van der Corput (11.27) yields the result. □

We are working with the decomposition $1_A = f_1 + f_2 \in \mathscr{H}_{rat} \oplus \mathscr{H}_{tot.erg}$. Lemma 11.28 implies that the Cesàro limit of $U^{n^2} f_2$ is zero. To complete the proof we analyze a similar expression for f_1.

11.29 Lemma. Suppose $1_A = f_1 + f_2$ as above. Then for every $\varepsilon > 0$ there exist $K = K(\varepsilon)$ such that for every N:

$$\left\langle \frac{1}{N}\sum_{n=1}^{N} U^{(Kn)^2} f_1\ ,\ f_1\right\rangle\ >\ \mu^2(A) - \varepsilon.$$

Assuming this result, for any $\varepsilon > 0$, Lemmas 11.29 and 11.28 show that there exists K such that:

$$\left\langle \frac{1}{N}\sum_{n=1}^{N} U^{(Kn)^2} 1_A\ ,\ 1_A\right\rangle\ >\ \mu^2(A) - \varepsilon.$$

From this we can prove that the squares form a set of recurrence for $(X, \mathcal{F}, \mu, T)$ because, when ε is small enough the inequality above implies:

$$\mu(A \cap T^{-n^2} A) = \langle U^{n^2} 1_A, 1_A\rangle > 0 \quad \text{for infinitely many values of } n.$$

Proof of Lemma 11.29. By Lemma 11.26, we may express $f_1 = \sum_{i=1}^{\infty} g_i$ where for each i, $U^i g_i = \lambda_i g_i$ where λ_i is a root of unity. Combine those summands where $\lambda_i = 1$ and relabel so that $Ug_j = g_j$ only when $j = 1$. Since U is unitary, g_j is orthogonal to 1_X for every $j > 1$. (Eigenvectors with different eigenvalues are orthogonal.)

We know $g_1 \in \mathscr{H}_{inv}$, and we split off the constant component: $g_1 = c1_X + \widetilde{g}_1$ where c is constant, $\widetilde{g}_1 \in \mathscr{H}_{inv}$, and $\widetilde{g}_1$ is orthogonal to 1_X. Therefore $c = \langle g_1, 1_X\rangle = \langle f_1, 1_X\rangle$. Since $f_2 \in \mathscr{H}_{tot.erg}$ is also orthogonal to 1_X, we find that $c = \langle f_1 + f_2, 1_X\rangle = \langle 1_A, 1_X\rangle = \mu(A)$. Therefore $f_1 = \mu(A)1_X + \widetilde{g}_1 + \sum_{j=2}^{\infty} g_j$, and it follows that:

$$||f_1|| \geq \mu(A).$$

Now approximate f_1 with a finite sum. Given $\varepsilon > 0$ there is $k \in \mathbb{N}$ such that $f_\varepsilon = \sum_{j=1}^{k} g_j$ satisfies $||f_1 - f_\varepsilon|| < \varepsilon$. Let $K = K_\varepsilon$ be a common multiple of the orders of λ_j for every j in that sum. Then $U^K f_\varepsilon = f_\varepsilon$.

Define $\ell = \frac{1}{N}\sum_{n=1}^{N} U^{(Kn)^2} f_1$. The Lemma will be proved if we can show that:

$$\langle \ell, f_1\rangle > \mu^2(A) - \varepsilon.$$

Note that $||\ell - f_\varepsilon|| = \left|\left|\frac{1}{N}\sum_{n=1}^{N} U^{(Kn)^2}(f_1 - f_\varepsilon)\right|\right| < \varepsilon$. Since f_1 and ℓ are both ε-close to f_ε we know that $||\ell - f_1|| < 2\varepsilon$, so that:

$$\big|\ \langle \ell, f_1\rangle - ||f_1||^2\ \big| = |\langle \ell - f_1, f_1\rangle| < ||\ell - f_1|| \cdot ||f_1|| < 2\varepsilon||f_1||.$$

Therefore $\quad \langle \ell, f_1\rangle\ >\ ||f_1||^2 - 2\varepsilon||f_1||\ >\ \mu^2(A) - 2\varepsilon||f_1||.$

This is almost the statement of the Lemma. Given $\varepsilon' > 0$ let $\varepsilon = \varepsilon'/(2||f_1||)$, apply the argument above, and conclude that $\langle \ell, f_1\rangle > \mu^2(A) - \varepsilon'$. □

This completes our proof of the Ergodic Sárközy Theorem 11.9.

One small problem with the proof as stated is that those Hilbert spaces are complex vector spaces but we acted as if all the functions were real valued. This possibility does not affect our proof because we observe that 1_A is a nonnegative real-valued function, and therefore its orthogonal projection f_1 to $\mathscr{H}_{rat}$ is also a nonnegative real valued function. This follows since the projection f_1 is found by optimizing the distance $d(g) = ||1_A - g||$ for $g \in \mathscr{H}_{rat}$.

The proof above actually yields a stronger statement than just saying that the squares form a set of recurrence.

11.30 Corollary. For a measure preserving system $(X, \mathcal{F}, \mu, T)$ as above, with $A \in \mathcal{F}$ with $\mu(A) > 0$, the set $\{n : \mu(A \cap T^{-n^2}A) > 0\}$ has positive upper density in $\mathbb{N}$.

Going further with this, the Cesàro convergence used above can be replaced by *uniform* Cesàro convergence, since $(n^2\alpha)$ is well distributed. Then we can prove that:

For every $\varepsilon > 0$ there exists $K = K(\varepsilon)$ such that for every $M < N$:

$$\frac{1}{N-M} \sum_{n=M}^{N-1} \mu(A \cap T^{(Kn)^2}A) \ > \ \mu^2(A) - \varepsilon.$$

Using that result one can prove:

11.31 Corollary. For every $\varepsilon > 0$ there exists $K > 0$ such that the set

$$\{n : \mu\big(A \cap T^{(Kn)^2}A\big) > \mu^2(A) - \varepsilon\} \text{ is syndetic.}$$

Consequently, the larger set $\{n : \mu(A \cap T^{n^2}A) > 0\}$ is syndetic.

Finally, one can apply Furstenberg's Correspondence Principle to prove:

11.32 Corollary. If $E \subseteq \mathbb{N}$ has positive upper density, $\overline{d}(E) > 0$, then:

$$\text{The set } \{n : n^2 = x - y \text{ for some } x, y \in E\} \text{ is syndetic.}$$

11.4 Potpourri of Patterns in Primes and Ramsey Theory Connections

Throughout this discussion we let P be the set of all prime numbers. The ancient Greeks proved that P is infinite, and in 1737, Euler proved the stronger result that the series $\displaystyle\sum_{p \in P} \frac{1}{p}$ diverges.

Here, we collect further prime number facts that emerged on the last day of class during discussions with the audience.

Bertrand's Postulate states that for $n \geq 2$, there is always a prime between n and $2n$. This was proved by Chebyshev in 1852.

In 1837 Dirichlet used analytic properties of L-functions to prove his famous theorem on primes in arithmetic progressions. For any a in $(\mathbb{Z}/m\mathbb{Z})^*$, Dirichlet proved that there are infinitely many primes $p \equiv a \pmod{m}$.

Moreover, those sets of primes have equal densities. Let $P_{a,m}$ be the primes in $a + m\mathbb{Z}$, that is:
$P_{a,m} = P \cap (a + m\mathbb{Z}) = \{p \in P : p \equiv a \pmod{m}\}$. Then for any $a, b \in (\mathbb{Z}/m\mathbb{Z})^*$:

$$\lim_{N\to\infty} \frac{\big|P_{a,m} \cap [1, N]\big|}{\big|P_{b,m} \cap [1, N]\big|} \ = \ 1.$$

The Prime Number Theorem provides an estimate for the number $\pi(x)$ of primes less than x:

$$\pi(x) \text{ is asymptotically equal to } \frac{x}{\log x}. \quad \text{That is: } \lim_{x\to\infty} \frac{\pi(x)}{x/\log x} = 1.$$

(Throughout this section, "log" stands for the natural logarithm.) Various conjectures about the asymptotic behavior of $\pi(x)$ had been made in the Nineteenth Century, and this powerful Theorem was proved (independently) by Jacques Hadamard and Charles Jean de la Vallée-Poussin in 1896, using properties of the Riemmann zeta function.

If we write p_n for the n^{th} prime number, the Prime Number Theorem can be reformulated to say: $p_n \sim n \log n$. That "asymptotic equality" means:

$$\lim_{n\to\infty} \frac{p_n}{n \log n} = 1.$$

11.33 Exercise. (a) Show that the asymptotic formulas above for $\pi(x)$ and for p_n are equivalent.
(b) Check that the Prime Number Theorem implies Euler's result: $\displaystyle\sum_{p\in P} \frac{1}{p} = \infty$.

The next several remarks relate to the question: Are there arbitrarily long arithmetic progressions of primes? By Definition 3.8, that's the same as: Is P an AP-rich set?

Before stating results about primes, we review some of the history of the study of AP-rich sets.

A precursor to this subject is the following theorem. An initial version was found by Leonard Eugene Dickson[3] [13] in 1909, and then improved by Issai Schur [36] in 1916.

11.34 Theorem (Dickson, Schur)**.** For any $n \in \mathbb{N}$ and for every large enough prime p, there exist $x, y, z \not\equiv 0 \pmod p$ such that $x^n + y^n \equiv z^n \pmod p$.

For his proof, Schur employed the following lemma.

11.35 Lemma (Schur)**.** For any $r \in \mathbb{N}$, there exists $N = N(r)$ such that for any r-coloring
$\{1, 2, \ldots, N\} = \displaystyle\bigcup_{i=1}^{r} C_i$, one of the C_i contains some $a,\ b,\ a+b$.

(This can also stated as: The equation $a + b = c$ is "partition-regular.")

Proof of Theorem 11.34, using Lemma 11.35.
Given n, choose p to be a prime larger than the N arising in Lemma 11.35 for n colors. Let $G = (\mathbb{Z}/p\mathbb{Z})^\times$ and let $G_n = \{g^n : g \in G\}$ be the subgroup of n^{th}-powers. If $d = \gcd(n, p-1)$ then $G_n = G_d$ is a subgroup of index d.(Why?) Color $G = \{1, 2, \ldots, p-1\}$ by the $d \le n$ cosets of G_n. Since $p > N$ in (11.35), there exist some $a, b, a+b$ all of the same color gG_n. In other words, there exist $a = gx^n, b = gy^n, a+b = gz^n$ for some $x, y, z \in G$. Then $x^n + y^n \equiv z^n \pmod p$. □

Schur's Lemma 11.35 follows quickly from Ramsey's Theorem, a combinatorial result published in 1930 by Frank Plumpton Ramsey [35]. (Ramsey died in 1930 at the age of 26.) See [21] for further discussions and extensions of those ideas. However, the full power of Ramsey's Theorem is not really needed to prove this Lemma. An elementary proof is presented, for example, in [37] on pp. 408-409.

11.36 Exercise. Prove Schur's Lemma by using Poincaré Recurrence. (For details see [2].)

Some years later, Schur conjectured that for any partition $\mathbb{N} = \displaystyle\bigcup_{i=1}^{r} C_i$, at least one of the C_i is AP-rich.

[3]For students in the Ross Program, note that Dickson was Arnold Ross's dissertation advisor.

This conjecture was popularized by Baudet, and was finally proved by van der Waerden in 1927, as stated in Theorem 3.7 above. See [40], [41].

The following year, Alfred Brauer [10] (a student of Schur) generalized this result and proved:

11.37 Theorem (Brauer)**.** If $\mathbb{N} = \bigcup_{i=1}^{r} C_i$, then at least one of the C_i has arbitrarily long arithmetic progressions having common difference also in C_i.

One nice aspect of Brauer's result is that it is a simultaneous extension of Schur's Lemma 11.35 and van der Waerden's Theorem 3.7.

To understand van der Waerden's Theorem more deeply, Paul Erdős and Paul Turán [16] conjectured that any subset of $\mathbb{N}$ with positive upper density must contain long arithmetic progressions:

11.38 Conjecture (Erdős-Turán 1936)**.** Every subset of $\mathbb{N}$ with positive upper density is AP-rich.

Partial results were proved by various mathematicians, but finally, many years later, Szemerédi [38] settled the Erdős-Turán conjecture:

11.39 Theorem (Szemerédi 1975)**.** If $E \subset \mathbb{N}$ and $\overline{d}(E) > 0$, then E is AP-Rich.

Szemerédi's proof involved intricate combinatorial arguments. Then in 1977 Furstenberg [19] discovered a wonderful ergodic theoretic proof of Szemerédi's Theorem 11.39. That proof uses the following Multiple Recurrence Theorem, generalizing Poincaré's result (10.14) about a single recurrence.

11.40 Theorem (Furstenberg)**.** For any measure preserving system $(X, \mathcal{F}, \mu, T)$, any $A \in \mathcal{F}$ with $\mu(A) > 0$, and any $k \in \mathbb{N}$, there exists $n \in \mathbb{N}$ such that

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

11.41 Exercise. Use (11.40) and Furstenberg's Correspondence Principle 11.11 to prove Szemerédi's Theorem 11.39.

Furstenberg's recurrence result 11.40 has a polynomial generalization [6]. We state a special case here.

11.42 Theorem (Bergelson-Leibman)**.** Suppose $(X, \mathcal{F}, \mu, T)$ is a measure preserving system in which T is invertible. Suppose $A \in \mathcal{F}$ with $\mu(A) > 0$, and $p_1(x), \ldots, p_m(x) \in \mathbb{Z}[x]$ are polynomials all with constant term zero. Then there exists $n \in \mathbb{N}$ such that

$$\mu\big(A \cap T^{p_1(n)}A \cap \cdots \cap T^{p_m(n)}A\big) > 0.$$

Although Szemerédi's Theorem and Furstenberg's proof were truly breakthroughs in the subject, they were still not sufficient to determine whether the set P of primes is AP-rich. (Check that P has zero upper density.)

Erdős made a stronger conjecture using a somewhat different notion of "largeness" for a set of integers.

11.43 Conjecture (Erdős)**.** If $E \subseteq \mathbb{N}$ and $\sum_{n \in E} \frac{1}{n} = \infty$, then E is AP-rich.

If (11.43) is proved true someday, it immediately yields the AP-richness of P, because Euler proved long ago that $\sum_{p \in P} \frac{1}{p} = \infty$.

11.44 Exercise. Show that (11.43) implies (11.38): If $\overline{d}(E) > 0$, then $\sum_{n \in E} \frac{1}{n} = \infty$.

Even though no one has yet proved Conjecture 11.43, in 2008 Ben Green and Terrence Tao [22] succeeded in proving that P is AP-rich. The Green-Tao Theorem is close in spirit to Szemerédi's theorem.

For $A \subseteq P$, define its *relative upper density* as: $\limsup_{N\to\infty} \dfrac{\big|A \cap \{p_1, p_2, \ldots, p_N\}\big|}{N}$.

11.45 Theorem (Green-Tao)**.** If $A \subseteq P$ has positive relative upper density then A is AP-rich.

The Green-Tao Theorem was subsequently generalized in 2008 by Tao and Ziegler [39] who considered "polynomial progressions" rather than just arithmetic progressions.

11.46 Theorem (Tao-Ziegler)**.** For $p_1(x), \ldots, p_m(x) \in \mathbb{Z}[x]$ all with constant term 0, there exist infinitely many integers $k, l \in \mathbb{Z}$ such that $k + p_1(l), \ldots, k + p_m(l)$ are all prime.

The Green-Tao theorem is the case when $p_i(x) = (i-1)x$.

Patterns in $P - 1$.

From a combinatorial viewpoint, the set $P - 1$ is even more interesting than the set P of prime numbers. Since P is AP-Rich, so is $P - 1$. Moreover, $P - 1$ exhibits interesting additive patterns.

11.47 Proposition. For any N there exist $x_1, x_2, \ldots, x_N \in P - 1$ such that any finite sum of distinct elements of $x_1, x_2, \ldots, x_N$ is also contained in $P - 1$.

For a proof, see [7]. □

11.48 Corollary. $P - 1$ is a set of recurrence.

Proof. Sets of recurrence were defined in (11.7). Choose N, find elements $x_1, \ldots, x_N \in P - 1$ as in (11.47), and let $n_k = x_1 + x_2 + \cdots + x_k$. Then for $i > j$ the number $n_i - n_j$ is a finite sum of x_j's, so it lies in $P - 1$. Then $P - 1$ contains arbitrarily large sets of differences, and the observation in (10.15) shows that $P - 1$ is a set of recurrence. □

All the results stated here for the set $P - 1$ also hold for $P + 1$. In particular, both $P - 1$ and $P + 1$ are sets of recurrence.

11.49 Exercise. If $a \neq \pm 1$, then $P + a$ is not a set of recurrence.

Moreover, $P - 1$ is actually a "set of multiple recurrence," meaning that in (11.40) the value n can be chosen from $P - 1$. (Similarly for $P + 1$.) See [7] for details.

There have been some recent news stories about "prime gaps." Those refer to new results related to the famous Twin Primes Conjecture:

$$p_{n+1} - p_n = 2 \quad \text{for infinitely many indices } n.$$

That ancient conjecture is still unresolved, but there has been recent progress. As of 2015 the best result is:

$$\liminf_{n\to\infty}(p_{n+1} - p_n) < 246.$$

In other words, there are infinitely many n such that $p_{n+1} - p_n < 246$. The breakthrough result in this direction was obtained by Yitang Zhang in 2013, who proved the result with 7×10^7 in place of 246 above. Many different mathematicians (in the "polymath project") worked to reduce that upper bound to 246, as announced in April 2014. Several general interest articles have appeared about Zhang's work on bounded gaps and some subsequent developments. For instance, see [44].

12 References

Hello! Welcome to the Department of Redundancy and Repetition Department. Hi! [4]

[1] V. Bergelson, Ergodic Ramsey theory. Logic and Combinatorics (Arcata, Calif., 1985), 63-87, *Contemp. Math.* **65**, Amer. Math. Soc., Providence, RI, 1987.

[2] V. Bergelson, A density statement generalizing Schur's theorem, *J. Combin. Theory Ser. A* **43** (1986) 338-343.

[3] V. Bergelson, Ergodic Ramsey theory – an update, London Math. Soc. Lecture Note Series **228** (1996) 1-61.

[4] V. Bergelson, The multifarious Poincaré recurrence theorem, *Descriptive set theory and dynamical systems* (edited by M. Foreman, A. Kechris, A. Louveau, B. Weiss), London Math. Soc. Lecture Note Series **277** (2000) 31-57.

[5] V. Bergelson, Some historical remarks and modern questions around the ergodic theorem, *Internat. Math. Nachrichten* **205** (2007) 1 - 10.
Posted at: `http://www.oemg.ac.at/IMN/imn205.pdf`

[6] Polynomial extensions of van der Waerden's and Szemerédi's theorems, *Journal of Amer. Math. Soc.* **9** (1996) 725-753.

[7] V. Bergelson, A. Leibman, and T. Ziegler, The shifted primes and the multidimensional Szemerédi and polynomial van der Waerden theorems, *C. R. Math. Acad. Sci. Paris* **349** (2011) 123-125.

[8] V. Bergelson and J. Moreira, Van der Corput's difference theorem: some modern developments, *Indag. Math.* (to appear)

[9] E. Borel, Les probabilités dénombrables et leurs applications arithmétiques, *Supplemento di rend. Circ. Mat. Palermo* **27** (1909) 247-271.

[10] A. Brauer, Über Sequenzen von Potenzresten, *S.-B. Preuss. Akad. Wiss.* (1928) 9-16.

[11] D. G. Champernowne, The construction of decimals normal in the scale of ten, *J. London Math. Soc.* **8** (1933) 254-260.

[12] J. G. van der Corput, Diophantische Ungleichungen. I. Zur Gleichverteilung modulo Eins, *Acta Math.* **56**(1) (1931) 373-456.

[13] L. E. Dickson, On the congruence $x^n + y^n \equiv z^n \pmod{p}$, *J. Reine Angew. Math.* **135** (1909) 134-141.

[14] V. Dragović and M. Radnović, Bicentennial of the great Poncelet theorem (1813-2013): current advances, *Bull. Amer. Math. Soc.* **51** (2014) 373–445.

[15] R. Ellis, Distal transformation groups, *Pac. J. Math* **8** (1958) 401-405.

[16] P. Erdős and P. Turán, On some sequences of integers, *J. London Math. Soc.* **11** (1936) 261-264.

[17] L. Flatto, *Poncelet's Theorem*, Amer. Math Soc., Providence, RI, 2009.

[18] H. Furstenberg, Disjointness in ergodic theory, minimal sets, and a problem in Diophantine approximation, *Math. Systems Theory* **1** (1967) 1-49.

[4] A greeting suggested by D. Shapiro.

[19] H. Furstenberg. Ergodic behavior of diagonal measures and a theorem of Szemerédi on arithmetic progressions. *J. d'Analyse Math.*, **31** (1977) 204-256.

[20] H. Furstenberg, *Recurrence in Ergodic Theory and Combinatorial Number Theory*, Princeton Univ. Press, 1981

[21] R. Graham, B. Rothschild, and J. Spencer, *Ramsey Theory*, Wiley, New York, 1980.

[22] B. Green and T. Tao, The primes contain arbitrarily long arithmetic progressions, *Annals of Mathematics* **167** (2008) 481-547.

[23] L. Halbeisen and N. Hungerbühler, A simple proof of Poncelet's theorem (on the occasion of its bicentennial), *Amer. Math. Monthly* **122** (2015) 537-551.

[24] G. Herglotz, Über Potenzreihen mit reelem Teil im Einheitskreis, *Sitzungber. Sächs. Akad. Wiss.* **63** (1911) 501-511.

[25] A. Y. Khinchin, *Three Pearls of Number Theory*, Graylock Press, 1952. (Translation of the 1948 Russian edition.) There is also a Dover reprint of this classic book.

[26] J. L. King, Three problems in search of a measure, *Amer. Math. Monthly* **101** (1994) 609-628.

[27] L. Kuipers and H. Niederreiter, *Uniform Distribution of Sequences*, John Wiley & Sons, 1974. [republished by Dover, 2002.] (See Chapter 3 for van der Corput's "Difference Theorem")

[28] J. Moreira, Equidistribution of polynomials, recurrence and van der Corput trick, Blog article posted at `https://joelmoreira.wordpress.com/2011/09/19/equidistribution-of-polynomials-recurrence-and-van-der-corput-trick/`
[Note. Joel Moreira is currently a graduate student at OSU.]

[29] J. von Neumann, Gleichmässig dichte Zahlenfolgen, *Mat. Fiz. Lapok* **32** (1925) 32-40.

[30] J. von Neumann, Proof of the quasi-ergodic hypothesis, *Proc. Nat. Acad. Sci. USA* **18** (1932), 70-82.

[31] K. Petersen, *Ergodic Theory*, Cambridge Studies in Advanced Math., **2**, Cambridge U. Press, 1983.

[32] H. Poincaré, Sur le problème des trois corps et les équations de la dynamique, *Acta Mathematica* **13** (1890) 1 - 270. For his Recurrence Theorem, see pp. 69 - 72.

[33] J.-V. Poncelet, *Traité des Propriétés Projectives des Figures*, Bachelie, Paris, 1822.

[34] R. Rado, Note on combinatorial analysis. *Proc. London Math. Soc.* (2) **48** (1943) 122-160.
In his comments on this paper in *Math Reviews* (MR0009007), P. Erdős refers to Grünwald's result. (Tibor Grünwald later changed his name to Tibor Gallai).

[35] F. P. Ramsey, On a problem of formal logic, *Proc. London Math. Soc.* **30** (1930) 264-286.

[36] I. Schur, Über die Kongruence $x^m + y^m \equiv z^m \pmod{p}$, *Jahresbericht der Deutschen Math.-Ver.* **25** (1916) 114-117.

[37] W. Sierpiński, *Elementary Theory of Numbers*, Warszawa 1964.

[38] E. Szemerédi, On sets of integers containing no k elements in arithmetic progression, *Acta Arith.* **27** (1975) 199-245.

[39] T. Tao and T. Ziegler, The primes contain arbitrarily long polynomial progressions, *Acta Mathematica* **201** (2008) 213-305.
Erratum: *Acta Mathematica* **210** (2013) 403-404.

[40] B.L. van der Waerden. Beweis einer baudetschen Vermutung, *Nieuw. Arch. Wisk.* **15** (1927) 212-216.

[41] B. L. van der Waerden, How the proof of Baudet's conjecture was found, *Studies in Pure Mathematics presented to Richard Rado*, L. Mirsky, ed., Academic Press, London, 1971, 251-260.

[42] S. Wagon, *The Banach Tarski Paradox*, Cambridge Univ. Press, 1985 (second edition 1993). [Discusses finitely additive measures and invariant means.]

[43] H. Weyl, Über die Gleichverteilung von Zahlen mod Eins, *Eins. Math. Ann.* **77**(3) (1916) 313-352.

[44] A. Wilkinson, The pursuit of beauty, *The New Yorker*, Feb. 2, 2015, as posted at `http://www.newyorker.com/magazine/2015/02/02/pursuit-beauty`