

CHAPTER 12

**Combinatorial and Diophantine Applications of
Ergodic Theory**

Vitaly Bergelson¹

*The Ohio State University, Columbus, OH 43210, USA
E-mail: vitaly@math.ohio-state.edu*

With Appendix A by A. Leibman²

*The Ohio State University, Columbus, OH 43210, USA
E-mail: leibman@math.ohio-state.edu*

With Appendix B by Anthony Quas³ and Máté Wierdl⁴

*Department of Mathematical Sciences, University of Memphis, 373 Dunn Hall, Memphis, TN 38152-3240, USA
E-mail: quasa@msci.memphis.edu, mw@csi.hu*

Contents

1. Introduction	747
1.1. Fermat's theorem over finite fields	747
1.2. Hilbert's theorem	749
1.3. IP sets and Hindman's finite sum theorem	750
1.4. Van der Waerden theorem: combinatorial and dynamical versions	752
1.5. Density Ramsey theory	754
1.6. Furstenberg's correspondence principle	755
1.7. Hales–Jewett theorem	756
1.8. Sárközy–Furstenberg theorem	758
2. Topological dynamics and partition Ramsey theory	762
2.1. Introduction	762
2.2. IP van der Waerden theorem	762

¹The author acknowledges support received from the National Science Foundation (USA) via grant DMS-0345350.

²Supported by NSF, grant DMS-0345350.

³A. Quas' research is partially supported by NSF grant #DMS-0200703.

⁴M. Wierdl's research is partially supported by NSF grant #DMS-0100577.

HANDBOOK OF DYNAMICAL SYSTEMS, VOL. 1B

Edited by B. Hasselblatt and A. Katok

© 2006 Elsevier B.V. All rights reserved

2.3. A simultaneous proof of van der Waerden and Hales–Jewett theorems	767
2.4. Polynomial van der Waerden theorem	772
2.5. Polynomial Hales–Jewett theorem	773
2.6. Nilpotent van der Waerden theorem	775
2.7. Nilpotent Hales–Jewett theorem	776
3. Dynamical, combinatorial, and Diophantine applications of $\beta\mathbb{N}$	777
3.1. Definition and properties of $\beta\mathbb{N}$	778
3.2. The semigroup operation in $\beta\mathbb{N}$	779
3.3. The analogy between idempotent ultrafilters and measure preserving systems. A new glimpse at Hindman’s theorem	782
3.4. Minimal idempotents	783
3.5. Ultrafilter proof of van der Waerden’s theorem	785
3.6. Central sets	786
3.7. Diophantine applications	791
4. Multiple recurrence	793
4.1. Introduction	793
4.2. Furstenberg’s ergodic Szemerédi theorem	793
4.3. An overview of multiple recurrence theorems	808
5. Actions of amenable groups	825
5.1. Generalities	825
5.2. Correspondence principle for countable amenable groups	829
5.3. Applications to multiplicatively large sets	834
5.4. Multiple recurrence for amenable groups	835
6. Issues of convergence	838
Acknowledgement	841
Appendix A. Host–Kra and Ziegler factors and convergence of multiple ergodic averages, by A. Leibman	841
A.1. Multiple ergodic averages	841
A.2. Construction of Host–Kra factors	843
A.3. Host–Kra factors for T^l	845
A.4. Characteristic factors for multiple averages	848
Acknowledgement	853
Appendix B. Ergodic averages along the squares, by A. Quas and M. Wierdl	853
B.1. Enunciation of the result	853
B.2. Subsequence lemma	854
B.3. Oscillation and an instructive example	855
B.4. Periodic systems and the circle method	857
B.5. The main inequality	860
B.6. Notes	864
Acknowledgement	864
References	864

1. Introduction

The main focus of this survey is the mutually perpetuating interplay between ergodic theory, combinatorics and Diophantine analysis.

Ergodic theory has its roots in statistical and celestial mechanics. In studying the long time behavior of dynamical systems, ergodic theory deals first of all with such phenomena as recurrence and uniform distribution of orbits.

Ramsey theory, a branch of combinatorics, is concerned with the phenomenon of preservation of highly organized structures under finite partitions.

Diophantine analysis concerns itself with integer and rational solutions of systems of polynomial equations.

To get a feeling about possible connections between these three quite distinct areas of mathematics, let us consider some examples.

1.1. Fermat's theorem over finite fields

Our first example is related to Fermat's last theorem. Given $n \in \mathbb{N}$, where \mathbb{N} , here and throughout this survey, represents the set of positive integers, and a prime p , consider the equation $x^n + y^n \equiv z^n \pmod{p}$. This equation (as well as its more general version $ax^n + by^n + cz^n \equiv 0 \pmod{p}$) was extensively studied in the 19th and early 20th centuries. (See [50, Chapter 26] for information on the early work and [118, Chapter XII] for more recent developments and extensions.) We are going to prove, with the help of ergodic and combinatorial considerations, the following theorem.

THEOREM 1.1. *For fixed $n \in \mathbb{N}$ and a large enough prime p , the polynomial $f(z, y) = z^n - y^n$ represents the finite field $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$. In other words, for any $c \in \mathbb{Z}_p$ there exist $z, y \in \mathbb{Z}_p^* = \mathbb{Z}_p \setminus \{0\}$, such that $c = z^n - y^n$.*

Putting $c = x^n$ immediately gives the following result, which was proved by Schur in 1916. (See also [49].)

COROLLARY 1.2 [126]. *For fixed $n \in \mathbb{N}$ and large enough prime p , the equation $x^n + y^n \equiv z^n \pmod{p}$ has nontrivial solutions.*

In the course of the proof of Theorem 1.1 we shall utilize the following classical fact due to F. Ramsey [117]. For a nice discussion which puts Ramsey's theorem into the perspective of *Ramsey theory*, see [72]. In what follows, $|A|$ denotes the cardinality of a set A .

THEOREM 1.3. *For any $n, r \in \mathbb{N}$ there exists a constant $c = c(n, r)$ such that if a set A satisfies $|A| \geq c$ and the set $[A]^2$ of two-element subsets of A is partitioned into r cells (or, as we will often say, is r -colored): $[A]^2 = \bigcup_{i=1}^r C_i$, then there exists a subset $B \subset A$ satisfying $|B| > n$ and such that for some i , $1 \leq i \leq r$, $[B]^2 \subset C_i$. (In this case we say that $[B]^2$ is monochromatic.)*