CHAPTER 12

Combinatorial and Diophantine Applications of Ergodic Theory

Vitaly Bergelson[1]
The Ohio State University, Columbus, OH 43210, USA
E-mail: vitaly@math.ohio-state.edu

With Appendix A by A. Leibman[2]
The Ohio State University, Columbus, OH 43210, USA
E-mail: leibman@math.ohio-state.edu

With Appendix B by Anthony Quas[3] and Máté Wierdl[4]
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]The author acknowledges support received from the National Science Foundation (USA) via grant DMS-0345350.
[2]Supported by NSF, grant DMS-0345350.
[3]A. Quas' research is partially supported by NSF grant #DMS-0200703.
[4]M. Wierdl's research is partially supported by NSF grant #DMS-0100577.

HANDBOOK OF DYNAMICAL SYSTEMS, VOL. 1B
Edited by B. Hasselblatt and A. Katok

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 $|A| \geqslant c$ 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, $1 \leqslant i \leqslant r$, $[B]^2 \subset C_i$. (In this case we say that $[B]^2$ is* monochromatic.)