CAMBRIDGE STUDIES IN ADVANCED MATHEMATICS 192

AN INTRODUCTION TO PROBABILISTIC NUMBER THEORY

Despite its seemingly deterministic nature, the study of whole numbers, especially prime numbers, has many interactions with probability theory, the theory of random processes and events. This surprising connection was first discovered around 1920, but in recent years, the links have become much deeper and better understood.

Aimed at beginning graduate students, this textbook is the first to explain some of the most modern parts of the story. Such topics include the Chebychev bias, universality of the Riemann zeta function, exponential sums, and the bewitching shapes known as Kloosterman paths. Emphasis is given throughout to probabilistic ideas in the arguments, not just the final statements, and the focus is on key examples over technicalities. The book develops probabilistic number theory from scratch, with short appendices summarizing the most important background results from number theory, analysis, and probability, making it a readable and incisive introduction to this beautiful area of mathematics.

Emmanuel Kowalski is Professor in the Mathematics Department of the Swiss Federal Institute of Technology, Zurich. He is the author of five previous books, including the widely cited *Analytic Number Theory* (2004) with H. Iwaniec, which is considered to be the standard graduate textbook for analytic number theory.

CAMBRIDGE STUDIES IN ADVANCED MATHEMATICS

All the titles listed below can be obtained from good booksellers or from Cambridge University Press. For a complete series listing, visit www.cambridge.org/mathematics.

Already Published

152 V. I. Paulsen & M. Raghupathi *An Introduction to the Theory of Reproducing Kernel Hilbert Spaces*

153 R. Beals & R. Wong *Special Functions and Orthogonal Polynomials*

154 V. Jurdjevic *Optimal Control and Geometry: Integrable Systems*

155 G. Pisier *Martingales in Banach Spaces*

156 C. T. C. Wall *Differential Topology*

157 J. C. Robinson, J. L. Rodrigo & W. Sadowski *The Three-Dimensional Navier-Stokes Equations*

158 D. Huybrechts *Lectures on K3 Surfaces*

159 H. Matsumoto & S. Taniguchi *Stochastic Analysis*

160 A. Borodin & G. Olshanski *Representations of the Infinite Symmetric Group*

161 P. Webb *Finite Group Representations for the Pure Mathematician*

162 C. J. Bishop & Y. Peres *Fractals in Probability and Analysis*

163 A. Bovier *Gaussian Processes on Trees*

164 P. Schneider *Galois Representations and* (φ, Γ)*-Modules*

165 P. Gille & T. Szamuely *Central Simple Algebras and Galois Cohomology (2nd Edition)*

166 D. Li & H. Queffelec *Introduction to Banach Spaces, I*

167 D. Li & H. Queffelec *Introduction to Banach Spaces, II*

168 J. Carlson, S. Müller-Stach & C. Peters *Period Mappings and Period Domains (2nd Edition)*

169 J. M. Landsberg *Geometry and Complexity Theory*

170 J. S. Milne *Algebraic Groups*

171 J. Gough & J. Kupsch *Quantum Fields and Processes*

172 T. Ceccherini-Silberstein, F. Scarabotti & F. Tolli *Discrete Harmonic Analysis*

173 P. Garrett *Modern Analysis of Automorphic Forms by Example, I*

174 P. Garrett *Modern Analysis of Automorphic Forms by Example, II*

175 G. Navarro *Character Theory and the McKay Conjecture*

176 P. Fleig, H. P. A. Gustafsson, A. Kleinschmidt & D. Persson *Eisenstein Series and Automorphic Representations*

177 E. Peterson *Formal Geometry and Bordism Operators*

178 A. Ogus *Lectures on Logarithmic Algebraic Geometry*

179 N. Nikolski *Hardy Spaces*

180 D.-C. Cisinski *Higher Categories and Homotopical Algebra*

181 A. Agrachev, D. Barilari & U. Boscain *A Comprehensive Introduction to Sub-Riemannian Geometry*

182 N. Nikolski *Toeplitz Matrices and Operators*

183 A. Yekutieli *Derived Categories*

184 C. Demeter *Fourier Restriction, Decoupling and Applications*

185 D. Barnes & C. Roitzheim *Foundations of Stable Homotopy Theory*

186 V. Vasyunin & A. Volberg *The Bellman Function Technique in Harmonic Analysis*

187 M. Geck & G. Malle *The Character Theory of Finite Groups of Lie Type*

188 B. Richter *Category Theory for Homotopy Theory*

189 R. Willett & G. Yu *Higher Index Theory*

190 A. Bobrowski *Generators of Markov Chains*

191 D. Cao, S. Peng & S. Yan *Singularly Perturbed Methods for Nonlinear Elliptic Problems*

An Introduction to Probabilistic Number Theory

EMMANUEL KOWALSKI
Swiss Federal Institute of Technology, Zürich

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE
UNIVERSITY PRESS

University Printing House, Cambridge CB2 8BS, United Kingdom

One Liberty Plaza, 20th Floor, New York, NY 10006, USA

477 Williamstown Road, Port Melbourne, VIC 3207, Australia

314–321, 3rd Floor, Plot 3, Splendor Forum, Jasola District Centre,
New Delhi – 110025, India

79 Anson Road, #06–04/06, Singapore 079906

Cambridge University Press is part of the University of Cambridge.

It furthers the University's mission by disseminating knowledge in the pursuit of education, learning, and research at the highest international levels of excellence.

www.cambridge.org
Information on this title: www.cambridge.org/9781108840965
DOI: 10.1017/9781108888226

First published 2021

A catalogue record for this publication is available from the British Library.

ISBN 978-1-108-84096-5 Hardback

Cambridge University Press has no responsibility for the persistence or accuracy of URLs for external or third-party internet websites referred to in this publication and does not guarantee that any content on such websites is, or will remain, accurate or appropriate.

Les probabilités et la théorie analytique des nombres, c’est la même chose.
paraphrase of Y. Guivarc’h, Rennes, July 2017

Cambridge University Press
978-1-108-84096-5 — An Introduction to Probabilistic Number Theory
Emmanuel Kowalski
Frontmatter
More Information

Contents

Preface *page* xi
Prerequisites and Notation xiii

1 Introduction 1
1.1 Presentation 1
1.2 How Does Probability Link with Number Theory Really? 2
1.3 A Prototype: Integers in Arithmetic Progressions 4
1.4 Another Prototype: The Distribution of the Euler Function 15
1.5 Generalizations 21
1.6 Outline of the Book 24

2 Classical Probabilistic Number Theory 26
2.1 Introduction 26
2.2 Distribution of Arithmetic Functions 26
2.3 The Erdős–Kac Theorem 31
2.4 Convergence without Renormalization 39
2.5 Final Remarks 45

3 The Distribution of Values of the Riemann Zeta Function, I 47
3.1 Introduction 47
3.2 The Theorems of Bohr–Jessen and of Bagchi 50
3.3 The Support of Bagchi's Measure 67
3.4 Generalizations 72

4 The Distribution of Values of the Riemann Zeta Function, II 75
4.1 Introduction 75
4.2 Strategy of the Proof of Selberg's Theorem 76
4.3 Dirichlet Polynomial Approximation 85
4.4 Euler Product Approximation 89
4.5 Further Topics 95

5 The Chebychev Bias 97
5.1 Introduction 97
5.2 The Rubinstein–Sarnak Distribution 98
5.3 Existence of the Rubinstein–Sarnak Distribution 102
5.4 The Generalized Simplicity Hypothesis 113
5.5 Further Results 123

6 The Shape of Exponential Sums 124
6.1 Introduction 124
6.2 Proof of the Distribution Theorem 129
6.3 Applications 139
6.4 Generalizations 143

7 Further Topics 144
7.1 Equidistribution Modulo 1 144
7.2 Roots of Polynomial Congruences and the Chinese Remainder Theorem 148
7.3 Gaps between Primes 151
7.4 Cohen–Lenstra Heuristics 152
7.5 Ratner Theory 153
7.6 And Even More . . . 155

***Appendix A* Analysis** 157
A.1 Summation by Parts 157
A.2 The Logarithm 158
A.3 Mellin Transform 159
A.4 Dirichlet Series 162
A.5 Density of Certain Sets of Holomorphic Functions 167

***Appendix B* Probability** 171
B.1 The Riesz Representation Theorem 171
B.2 Support of a Measure 172
B.3 Convergence in Law 174
B.4 Perturbation and Convergence in Law 177
B.5 Convergence in Law in a Finite-Dimensional Vector Space 182
B.6 The Weyl Criterion 187
B.7 Gaussian Random Variables 194
B.8 Sub-Gaussian Random Variables 197
B.9 Poisson Random Variables 199
B.10 Random Series 200
B.11 Some Probability in Banach Spaces 209

***Appendix C* Number Theory** 222
C.1 Multiplicative Functions and Euler Products 222
C.2 Additive Functions 226
C.3 Primes and Their Distribution 227
C.4 The Riemann Zeta Function 230
C.5 Dirichlet L-Functions 234
C.6 Exponential Sums 240

References 246
Index 252

Cambridge University Press
978-1-108-84096-5 — An Introduction to Probabilistic Number Theory
Emmanuel Kowalski
Frontmatter
More Information

Preface

The style of this book is a bit idiosyncratic. The results that interest us belong to number theory, but the emphasis in the proofs will be on the probabilistic aspects and on the interaction between number theory and probability theory. In fact, we attempt to write the proofs so that they use *as little arithmetic as possible*, in order to clearly isolate the crucial number-theoretic ingredients that are involved.

This book is quite short. We attempt to foster an interest in the topic by focusing on a few key results that are accessible and at the same time particularly appealing, in the author's opinion, without targeting an encyclopedic treatment of any. We also try to emphasize connections to other areas of mathematics – first, to a wide array of arithmetic topics, but also to some aspects of ergodic theory, expander graphs, and so on.

In some sense, the ideal reader of this book is a student who has attended at least one introductory advanced undergraduate or beginning graduate-level probability course, including especially the Central Limit Theorem, and maybe some aspects of Brownian motion, and who is interested in seeing how probability interacts with number theory. For this reason, there are almost no number-theoretic prerequisites, although it is helpful to have some knowledge of the distribution of primes.

Probabilistic number theory is currently evolving very rapidly, and uses more and more refined probabilistic tools and results. For many number theorists, we hope that the detailed and motivated discussion of basic probabilistic facts and tools in this book will be useful as a basic “toolbox”.

Acknowledgments. The first draft of this book was prepared for a course Introduction to Probabilistic Number Theory that I taught at ETH Zürich during the fall semester of 2015. Thanks to the students of the course for their interest, in particular to M. Gerspach, A. Steiger, and P. Zenz for sending corrections and to B. Löffel for organizing and preparing the exercise sessions.

Thanks to M. Burger for showing me Cauchy's proof of the Euler formula,

$$\sum_{n=1}^{+\infty}\frac{1}{n^2}=\frac{\pi^2}{6},$$

in Exercise 1.3.4. Thanks to V. Tassion for help with the proof of Proposition B.11.11 and to G. Ricotta and E. Royer for pointing out a small mistake in [79].

Thanks to M. Radziwiłł and K. Soundararajan for sharing their proof [95] of Selberg's Central Limit Theorem for $\log|\zeta(\frac{1}{2}+it)|$, which was then unpublished.

This work was partially supported by the DFG-SNF lead agency program grant 200020L_175755.

Prerequisites and Notation

The basic requirements for most of this text are standard introductory graduate courses in algebra, analysis (including Lebesgue integration and complex analysis), and probability. Of course, knowledge and familiarity with basic number theory (for instance, the distribution of primes up to the Bombieri–Vinogradov Theorem) are helpful, but we review in Appendix C all the results that we use. Similarly, Appendix B summarizes the notation and facts from probability theory that are the most important for us.

We will use the following notation:

(1) For subsets Y_1 and Y_2 of an arbitrary set X, we denote by $Y_1 - Y_2$ the difference set, that is, the set of elements $x \in Y_1$ such that $x \notin Y_2$.

(2) A locally compact topological space is always assumed to be separated (i.e., Hausdorff), as in Bourbaki [15].

(3) For a set X, $|X| \in [0, +\infty]$ denotes its cardinal, with $|X| = \infty$ if X is infinite. There is no distinction in this text between the various infinite cardinals.

(4) If X is a set and f, g two complex-valued functions on X, then we write synonymously $f = O(g)$ or $f \ll g$ to say that there exists a constant $C \geqslant 0$ (sometimes called an "implied constant") such that $|f(x)| \leqslant Cg(x)$ for all $x \in X$. Note that this implies that in fact $g \geqslant 0$. We also write $f \asymp g$ to indicate that $f \ll g$ and $g \ll f$.

(5) If X is a topological space, $x_0 \in X$ and f and g are functions defined on a neighborhood of x_0, with $g(x) \neq 0$ for x in a neighborhood of x_0, then we say that $f(x) = o(g(x))$ as $x \to x_0$ if $f(x)/g(x) \to 0$ as $x \to x_0$, and that $f(x) \sim g(x)$ as $x \to x_0$ if $f(x)/g(x) \to 1$.

(6) We write $a \mid b$ for the divisibility relation "a divides b"; we denote by (a, b) the gcd of two integers a and b, and by $[a, b]$ their lcm.

(7) Usually, the variable p will always refer to prime numbers. In particular, a series $\sum_p(\cdots)$ refers to a series over primes (summed in increasing order, in case it is not known to be absolutely convergent), and similarly for a product over primes.

(8) We denote by $\mathbf{F}_p$ the finite field $\mathbf{Z}/p\mathbf{Z}$, for p prime, and more generally by $\mathbf{F}_q$ a finite field with q elements, where $q = p^n$, $n \geqslant 1$, is a power of p. We will recall the properties of finite fields when we require them.

(9) For a complex number z, we write $e(z) = e^{2i\pi z}$. If $q \geqslant 1$ and $x \in \mathbf{Z}/q\mathbf{Z}$, then $e(x/q)$ is well defined by taking any representative of x in $\mathbf{Z}$ to compute the exponential.

(10) If $q \geqslant 1$ and $x \in \mathbf{Z}$ (or $x \in \mathbf{Z}/q\mathbf{Z}$) is an integer that is coprime to q (or a residue class invertible modulo q), we sometimes denote by $\bar{q}$ the inverse class such that $x\bar{x} = 1$ in $\mathbf{Z}/q\mathbf{Z}$. This will always be done in such a way that the modulus q is clear from context, in the case where x is an integer.

(11) Given a probability space $(\Omega, \Sigma, \mathbf{P})$, we denote by $\mathbf{E}(\cdot)$ (resp. $\mathbf{V}(\cdot)$) the expectation (resp. the variance) computed with respect to $\mathbf{P}$. It will often happen that we have a sequence $(\Omega_{\mathrm{N}}, \Sigma_{\mathrm{N}}, \mathbf{P}_{\mathrm{N}})$ of probability spaces; we will then denote by $\mathbf{E}_{\mathrm{N}}$ or $\mathbf{V}_{\mathrm{N}}$ the respective expectation and variance with respect to $\mathbf{P}_{\mathrm{N}}$.

(12) Given a measure space (Ω, Σ, μ) (not necessarily a probability space), a set Y with a σ-algebra Σ' and a measurable map $f : \Omega \longrightarrow \mathrm{Y}$, we denote by $f_*(\mu)$ (or sometimes $f(\mu)$) the image measure on Y; in the case of a probability space, so that f is seen as a random variable on Ω, this is the probability law of f seen as a "random Y-valued element." If the set Y is given without specifying a σ-algebra, we will view it usually as given with the σ-algebra generated by sets $\mathrm{Z} \subset \mathrm{Y}$ such that $f^{-1}(\mathrm{Z})$ belongs to Σ.

(13) As a typographical convention, we will use sans-serif fonts like X to denote an *arithmetic* random variable and more standard fonts (like X) for "abstract" random variables. When using the same letter, this will usually mean that somehow the "purely random" X is the "model" of the arithmetic quantity X.