STUDENT MATHEMATICAL LIBRARY
Volume 6

The Prime Numbers and Their Distribution

Gérald Tenenbaum
Michel Mendès France

AMS
American Mathematical Society

http://dx.doi.org/10.1090/stml/006

Selected Titles in This Series

Volume

6 **Gérald Tenenbaum and Michel Mendès France**
The prime numbers and their distribution
2000

5 **Alexander Mehlmann**
The game's afoot! Game theory in myth and paradox
2000

4 **W. J. Kaczor and M. T. Nowak**
Problems in mathematical analysis I: Real numbers, sequences and series
2000

3 **Roger Knobel**
An introduction to the mathematical theory of waves
2000

2 **Gregory F. Lawler and Lester N. Coyle**
Lectures on contemporary probability
1999

1 **Charles Radin**
Miles of tiles
1999

This page intentionally left blank

The Prime Numbers and Their Distribution

This page intentionally left blank

STUDENT MATHEMATICAL LIBRARY
Volume 6

The Prime Numbers and Their Distribution

Gérald Tenenbaum
Michel Mendès France

Translated by
Philip G. Spain

Originally published in French, as
Les Nombres Premiers
Que sais-je?, No. 571, 1997 ed.

Translated from the French by Philip G. Spain

2000 *Mathematics Subject Classification.* Primary 11Nxx, 11N05;
Secondary 11–01, 11A41, 11Mxx.

Library of Congress Cataloging-in-Publication Data

Tenenbaum, Gerald.
[Nombres premiers. French]
The prime numbers and their distribution / Gérald Tenenbaum, Michel Mendès France ; translated by Philip G. Spain.
p. cm. — (Student mathematical library, ISSN 1520-9121 ; v. 6)
Includes bibliographical references.
ISBN 0-8218-1647-0 (soft cover : alk. paper)
1. Numbers, Prime. I. Mendès France, Michel, 1936– II. Title. III. Series.
QA246.T3614 2000
512′.72—dc21 00-020740

10 9 8 7 6 5 4 3 2 05 04 03 02 01

Contents

Preface to the English Edition ix

Preface to the French Edition xi

Notation and conventions xvii

Chapter 1. Genesis: From Euclid to Chebyshev 1

§0. Introduction 1

§1. Canonical decomposition 4

§2. Congruences 5

§3. Cryptographic intermezzo: public key systems 8

§4. Quadratic residues 11

§5. Return to the infinitude of the set of primes 12

§6. The sieve of Eratosthenes 14

§7. The Chebyshev theorems 16

§8. Mertens' theorems 21

§9. Brun's sieve and the twin prime conjecture 25

Chapter 2. The Riemann Zeta Function 29

§0. Introduction 29

§1. Euler's product 30

§2. Analytic continuation 32

§3. The line $\sigma = 1$ and the prime number theorem 38

§4. The Riemann hypothesis 42

§5. Arithmetic consequences of information on the zeros 46

Chapter 3. Stochastic Distribution of Prime Numbers 51

§0. Introduction 51

§1. Arithmetic progressions 52

§2. Cramér's model 61

§3. Uniform distribution modulo one 67

§4. Geometric vision 72

Chapter 4. An Elementary Proof of the Prime Number Theorem 77

§0. Introduction 77

§1. Integration by parts 80

§2. Convolution of arithmetic functions 81

§3. The Möbius function 85

§4. The mean value of the Möbius function and the prime number theorem 88

§5. Integers free of large, or small, prime factors 92

§6. Dickman's function 96

§7. Daboussi's proof, revisited 99

Chapter 5. The Major Conjectures 105

Further reading 113

Preface to the English Edition

The French edition of this book was first published in 1997 by *Presses Universitaires de France* in a series called "Que sais-je?" (*What do I know?*) alluding to Michel de Montaigne's own questioning. The series, which was devised from the start as a paperback encyclopedia, contains to date about 3500 titles, each book consisting of exactly $2^7 = 128$ pages. The topics cover all subjects: law, science, philosophy, art, history, *etc.* Amongst these there are only a few books discussing mathematics.

The editorial policy is rather unusual and worth mentioning. When an author dies, or simply loses interest in revising his monograph, the publisher asks a new specialist to write a book on the same subject, with the same title and the same number in the series. Apart from these constraints, no specific directive is imposed on the new author, who is therefore free to treat the matter according to his own conception of the subject.

In 1953, Émile Borel wrote a first version of *Les nombres premiers* and died three years later. Jean Itard wrote a second version in 1969 and died ten years later. We, the new authors, published ours in 1997 and, as far as we know, we seem to be in good health... And we dearly hope our book will last a long time!

We wish to express here our gratitude to Andrew Granville, who first proposed the idea of a translation to the American Mathematical Society, and who is also present in this book, amongst many other number theorists, through his mathematical results. Joan Mendès France and Mohan Nair greatly helped us at various stages of the groundwork of this edition: we thank them warmheartedly. And, of course, we take full responsibility for any mistakes or shortcomings!

Preface to the French Edition

This book is dedicated to the memory of Paul Erdös, who left us in September 1996, at the very moment when we completed the writing of the first edition. He was an uncle to us (and so his friends called him) and a master. A giant of mathematics disappeared: his influence will be felt profoundly in the centuries to come.

Number 571 of the collection *Que sais-je?* already has a history. The first edition dates from 1953. It was written by Émile Borel, a mathematician of great breadth, who profoundly influenced the theories of analysis, probability and mathematical physics. Some of his innovative works dealt with applications of probability to number theory, though, regrettably, he did not mention them in his monograph *Les nombres premiers.* Using randomness to study certainty may seem somewhat surprising. It is, however, one of the deepest contributions of our century to mathematics in general and to the theory of numbers in particular.

In 1969, Jean Itard took over from Borel and brought out a new text, devoting the major part to algebraic methods, which are certainly more accessible to a broad audience.

We have deliberately chosen to radically distance ourselves from our two predecessors by taking up a daunting challenge, namely to introduce the modern analytic theory of prime numbers — excluding, however, very recent contributions from the theory of modular forms.

In tackling the age-old questions — are there many prime numbers?, how are they distributed?, *etc.* — this field has blossomed unprecedentedly over the last hundred years, notably because of its interactions with probability theory.

Tables of prime numbers display a chaotic aspect whose apparent disorder somewhat resembles classical random models arising, for example, from physical phenomena. And here is exactly the purpose of this little book: to describe, and then to try to understand, how a sequence so precisely determined as that of prime numbers can incorporate so great a share of randomness.

Let us take this point a little further. Total randomness, chaos, is infinite complexity. Besides, the complexity of an integer obviously grows with its size: is the number $2^{6972593} - 1$ prime?[1] In the neighbourhood of infinity, the sequence of integers, and therefore that of prime numbers, contains randomness. Current research in modern analytic number theory tries to account for this aspect.

Physicists and philosophers continue to debate the existence of "hidden variables". The Copenhagen School, with Niels Bohr, defends the thesis that the subatomic world is governed by chance. Einstein, for his part, dreams of a totally deterministic sub-subatomic explanation. Could it be that the sequence of prime numbers serves as a model for the ideas of Einstein, who maintained that God does not play dice, while the eminent number theorist Mark Kac professed the opinion that prime numbers play a game of chance?

The dialectic pair order/disorder has occupied number theorists since Legendre and Gauss conjectured a harmonious distribution for the prime numbers, namely that the n^{th} prime number is approximately equal to $n \log n$.[2] Such regularity in randomness is hardly surprising: what could be more unpredictable than the toss of a coin,

[1] Yes, according to Hajratwala, Woltman and Kurowski (1999).

[2] This was proved by Jacques Hadamard and Charles de La Vallée-Poussin in 1896, just over one hundred years ago.

even though the probability governing the event is consistently $\frac{1}{2}$ and never budges?

We have chosen to describe these phenomena from a historical perspective, following the gradual development of the philosophy — that is, working out of basic conceptual representation — of prime number theory. Chapters 1, 2 and 4 are mainly devoted to regularity results, while Chapter 3 essentially deals with random aspects of the distribution of prime numbers. In Chapter 5 we describe the principal conjectures which underpin the theory, and we eventually come to understand that this dichotomy is merely apparent. Indeed, chance and necessity intertwine harmoniously to produce structure, and each of these strands clarifies and explains the other.

Every choice entails restriction. Our narrative approach also has its pitfalls and shortcomings. Breaking deliberately (some will say scandalously) with a century-old tradition in this type of work, we do not provide a table of prime numbers[3] and we do not give our favourite proof of the law of quadratic reciprocity. On a more serious note, we shall not discuss the various and deep generalizations of prime numbers in commutative algebra, *e.g.* prime ideals in number fields, irreducible polynomials over a ring or a finite field, *etc.*For this one may consult the classical books available in French.[4] We also ignore, almost totally, the "divisor" aspect of prime numbers, even though it provides a singular field of investigation for probabilistic methods in number theory.[5] Finally, we shall touch only very briefly (in Chapter 1, §3) on the cryptographic and algorithmic aspects of the theory, whose striking applications have, in recent years, been well popularized.[6]

Science as a whole, and indeed mathematics, has an ever increasing place in general culture. Besides, there is no shortage of "pleasing

---

[3] A lacuna which can easily be compensated for by using a desk calculator.

[4] And in English as well: see, for example: P. Samuel, *Algebraic theory of numbers*, Houghton Mifflin Co., 1970; Z.I. Borevitch & I.R. Shafarevitch, *Number Theory*, Academic Press, 1966; J.-P. Serre, *Local fields*, Graduate Texts in Mathematics 67, Springer-Verlag, 1979.

[5] This point of view has been developed in several recent works, in particular: P.D.T.A. Elliott, *Probabilistic number theory* (2 vol.), Springer Verlag, 1979-1980; R.R. Hall & G. Tenenbaum, *Divisors*, Cambridge University Press, 1988.

[6] For more on this, see the book of G. Robin, *Algorithmique et cryptographie*, SMAI, coll. "Ellipses", 1991.

and delectable"[7] expository works, some quite remarkable,[8] which are devoted to spectacular aspects of prime numbers. We have therefore chosen to follow a different path with the deliberate intention to aim a little higher than is usual in a work designed for a broader readership. We are aware that certain developments will seem difficult — they are. We have sometimes preferred a short calculation (the mathematician's sketch) to a long explanation, and the style is purposely condensed, even to the extent of being in some places allusive. This seemed necessary to us in order to clarify some of the essential arguments. Thus we hope that attentive and tenacious readers will satisfy their curiosity with locally complete proofs — it was with this intention in mind that we drafted Chapter 4, which is essentially self-contained. But we would also encourage more hurried readers, or those less interested in entering into details, to read this book "diagonally", granted it is true that only definitions matter, provided one understands them, and these resonate with each other through intrinsic logic. The rest is mere chatter.

In contrast with analytic reading, *i.e.* not going to line $n+1$ until line n is understood and assimilated, we would support a more synthetic approach (made possible precisely because of the conciseness of the presentation), a *glissando,* where the leading string is always heard.

Once an overall understanding has been attained, nothing prevents the reader (and, as will have been understood, it is indeed necessary for further progress) from going back, pen in hand, and inspecting the rigour, if not the roughness, of the proofs. The game is worth the candle.

This book is not easy, yet through its mystery we hope it will convey the hidden pleasure of poetry. Out of complexity is born the dream. Neither Stéphane Mallarmé nor Umberto Eco would disagree.

We have relied, at several stages in the writing of this book, on help from a variety of friendly sources. We wish to express here our special gratitude to Jean-Paul Allouche, Jean-Philippe Anker, Michel

[7] To use the expression of Bachet (1612).

[8] The exhaustive *Nombres premiers: mystères et records*, of P. Ribenboim, PUF 1994, is one of them.

Balazard, Daniel Barlet, Régis de La Bretèche, Éric Charpentier, Hédi Daboussi, Cécile Dartyge, Jean-Marc Deshouillers, Jean-Claude Fort, Andrew Granville, Jerzy Kaczorowski, Bernard Landreau, Pierre Marchand, Gérard Mathieu, Jean-Louis Nicolas, Emmanuel Pedon, Patrick Sargos, Jacques Sicherman, André Stef, Jie Wu, and Paul Zimmermann.

Nancy and Bordeaux, September 1996,

G. T. & M. M.F.

This page intentionally left blank

Notation and conventions

We indicate here the main notation and conventions used generally in this work. Those which appear only in a chapter or section are defined *in situ.*

The letter $\mathbb{N}$ denotes the set of natural numbers $\{1, 2, \dots\}$, and $\mathcal{P}$ that of prime numbers. The sets of integers, real numbers and complex numbers are denoted respectively by $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$. The letter p, with or without a subscript, always denotes an element of $\mathcal{P}$. We write $a \mid b$ (resp. $a \nmid b$) to indicate that a divides (resp. does not divide) b, and $p^\nu \| a$ to mean that $p^\nu | a$ but $p^{\nu+1} \nmid a$.

The gcd of two integers a, b is denoted by (a, b). Integers a and b with $(a, b) = 1$ are called coprime.

The number of elements of a finite set A is denoted, according to circumstances, by $|A|$ or $\sum_{a \in A} 1$. We denote by $P^+(a)$ (resp. $P^-(a)$) the greatest (resp. the least) prime factor of an integer $a \in \mathbb{N}$, with the convention $P^+(1) = 1$, $P^-(1) = \infty$.

The Napierian logarithm is denoted by log .[9] The iterates log log, log log log, *etc.*, are denoted by $\log_2$, $\log_3$, *etc.*Euler's constant γ is

[9] $\log a$ is thus, for $a \geqslant 1$, the area of the region bounded by the axes $x = 1$, $x = a$, $y = 0$ and the curve $y = 1/x$. When a is "large", $\log a \sim \sum_{n \leqslant a} 1/n$.

defined as the limit

$$\gamma = \lim_{N\to\infty} \Big(\sum_{n\leqslant N} 1/n - \log N \Big),$$

with approximate value $\gamma \approx 0.577215664$. It should be noted, however, that in Chapter 2 we follow traditional usage in also letting γ denote the imaginary part of a generic zero of the Riemann zeta function.

The integer part and fractional part of a real number x are indicated by $[x]$ and $\{x\}$ respectively. Thus

$$[5/3] = 1, \quad \{-3.15\} = 0.85.$$

The assignment sign $:=$ indicates that the term on the left is defined by that on the right.

The *logarithmic integral* function is defined by

$$\mathrm{li}(x) := \int_2^x \frac{\mathrm{d}t}{\log t} \qquad (x \geqslant 2).$$

When the letter s denotes a complex number we define its real and imaginary parts implicitly by $s = \sigma + i\tau$.

Given two functions f, g of a real or complex variable, we use the Landau notation, $f = O(g)$, or that of Vinogradov, $f \ll g$, interchangeably, to mean that there is a positive constant C such that $|f| \leqslant Cg$ on the common domain of definition of f and g. Possible dependence of C on a parameter α may be indicated in the form $f = O_\alpha(g)$ or $f \ll_\alpha g$. The Landau notation $f = o(g)$ is used in its usual sense of $\lim f/g = 0$.[10] We write $f \sim g$ to indicate that $\lim f/g = 1$.

The *indicator function* of a set A is the function which is equal to 1 on A and to 0 on its complement. Finally, $\mathcal{C}^k[a,b]$ denotes the space of k times continuously differentiable functions on the interval $[a,b]$.

Further, we shall often use the following manipulation to estimate a weighted mean, with complex coefficients a_n, of values at integer

[10] So $O(1)$ denotes a bounded quantity and $o(1)$ a quantity which tends to 0.

arguments of a function $f \in \mathcal{C}^1[1, x]$:

$$\sum_{1 \leqslant n \leqslant x} a_n f(n) = \sum_{1 \leqslant n \leqslant x} a_n \Big\{ f(x) - \int_n^x f'(t)\,\mathrm{d}t \Big\}$$
$$= f(x) \sum_{1 \leqslant n \leqslant x} a_n - \int_1^x f'(t) \Big\{ \sum_{1 \leqslant n \leqslant t} a_n \Big\}\,\mathrm{d}t.$$

This page intentionally left blank

Further reading

E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, Astérisque 18, Société Mathématique de France 1974, 87 pp.

H. Cohen, *A course in computational algebraic number theory*, Graduate Texts in Mathematics 138, Springer-Verlag 1993, xxi+534 pp.

H. Davenport, *Multiplicative number theory*, Springer, New York, Heidelberg, Berlin 1980, second edition revised by H. L. Montgomery, xiii+177 pp.

H. M. Edwards, *Riemann's zeta function*, Academic Press, New York, London 1974, xiii+315 pp.

P. D. T. A. Elliott, *Probabilistic number theory: mean value theorems*, Grundlehren der Math. Wiss. 239, Springer-Verlag, New York, Berlin, Heidelberg, 1979, xxii+359 pp.

P. D. T. A. Elliott, *Probabilistic number theory: central limit theorems*, Grundlehren der Math. Wiss. 240, Springer-Verlag, New York, Berlin, Heidelberg, 1980, xviii+341 pp.

W. J. Ellison & M. Mendès France, *Les nombres premiers*, Hermann, Paris, 1975, xiv+442 pp.

H. Halberstam & H.-E. Richert, *Sieve methods*, London Mathematical Society Monographs 4, Academic Press, London, New York, San Francisco 1974, xiii+364 pp., erratum slip 2 pp.

R. R. Hall & G. Tenenbaum, *Divisors*, Cambridge Tracts in Mathematics 90, Cambridge University Press 1988, xvi+167 pp.

G. H. Hardy & E. M. Wright, *An introduction to the theory of numbers*, Oxford 1938, fifth edition 1979, xvi+426 pp.

M. N. Huxley, *The distribution of prime numbers*, Oxford Mathematical Monographs, Oxford 1972, x+128 pp.

A. E. Ingham, *The distribution of prime numbers*, Cambridge University Press, first edition 1932, reprint 1990, xviii+114 pp.

A. Ivić, *The Riemann zeta-function*, John Wiley, New York, Chichester, Brisbane, Toronto, Singapore 1985, xvi+517 pp.

H. Iwaniec, *Introduction to the spectral theory of automorphic forms*, Biblioteca de la Revista Matematica Iberoamericana, Madrid 1995, xiii+247 pp.

M. Kac, *Statistical independence in probability, analysis and number theory*, fourth printing, Carus Mathematical Monographs 12, Mathematical Association of America, distributed by John Wiley & Sons 1972, xiv+94 pp.

E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen* (2 vols.), Teubner, Leipzig 1909; third edition : Chelsea, New York 1974, xxv+1001 pp.

H. L. Montgomery, *Ten lectures on the interface between analytic number theory and harmonic analysis*, CBMS Regional Conferences Series in Mathematics 84, American Mathematical Society, Providence, Rhode Island 1994, xii+220 pp.

I. Niven, H. S. Zuckerman, H. L. Montgomery, *An introduction to the theory of numbers*, John Wiley New York, Chichester, Brisbane, Toronto, Singapore 1991, xiii+527 pp.

J.-P. Serre, *A course in arithmetic*, Graduate Texts in Mathematics 7, Springer-Verlag, New York, Heidelberg, Berlin 1978, ix+115 pp.

G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics 46, Cambridge University Press 1995, xv+448 pp.

E. C. Titchmarsh, *The theory of the Riemann zeta-function*, Oxford 1951, second edition 1986, revised by D. R. Heath-Brown, x+412 pp.

R. C. Vaughan, *The Hardy–Littlewood method*, Cambridge Tracts in Mathematics 125, second edition, Cambridge University Press 1997, xiii+232 pp.

The Prime Numbers and Their Distribution

Gérald Tenenbaum and Michel Mendès France

One notable new direction this century in the study of primes has been the influx of ideas from probability. The goal of this book is to provide insights into the prime numbers and to describe how a sequence so tautly determined can incorporate such a striking amount of randomness.

The book opens with some classic topics of number theory. It ends with a discussion of some of the outstanding conjectures in number theory. In between are an excellent chapter on the stochastic properties of primes and a walk through an elementary proof of the Prime Number Theorem.

This book is suitable for anyone who has had a little number theory and some advanced calculus involving estimates. Its engaging style and invigorating point of view will make refreshing reading for advanced undergraduates through research mathematicians.

ISBN 0-8218-1647-0

9 780821 816479

STML/6