MULTIPLICATIVE NUMBER THEORY I: CLASSICAL THEORY

Prime numbers are the multiplicative building blocks of natural numbers. Understanding their overall influence and especially their distribution gives rise to central questions in mathematics and physics. In particular their finer distribution is closely connected with the Riemann hypothesis, the most important unsolved problem in the mathematical world. Assuming only subjects covered in a standard degree in mathematics, the authors comprehensively cover all the topics met in first courses on multiplicative number theory and the distribution of prime numbers. They bring their extensive and distinguished research expertise to bear in preparing the student for intelligent reading of the more advanced research literature. The text, which is based on courses taught successfully over many years at Michigan, Imperial College and Pennsylvania State, is enriched by comprehensive historical notes and references as well as over 500 exercises.

Hugh Montgomery is a Professor of Mathematics at the University of Michigan.

Robert Vaughan is a Professor of Mathematics at Pennsylvannia State University.

CAMBRIDGE STUDIES IN ADVANCED MATHEMATICS

All the titles listed below can be obtained from good booksellers of from Cambridge University Press. For a complete series listing visit:
http://www.cambridge.org/series/sSeries.asp?code=CSAM

Already published

70 R. Iorio & V. Iorio *Fourier analysis and partial differential equations*
71 R. Blei *Analysis in integer and fractional dimensions*
72 F. Borceaux & G. Janelidze *Galois theories*
73 B. Bollobás *Random graphs*
74 R. M. Dudley *Real analysis and probability*
75 T. Sheil-Small *Complex polynomials*
76 C. Voisin *Hodge theory and complex algebraic geometry, I*
77 C. Voisin *Hodge theory and complex algebraic geometry, II*
78 V. Paulsen *Completely bounded maps and operator algebras*
79 F. Gesztesy & H. Holden *Soliton Equations and Their Algebro-Geometric Solution, I*
81 S. Mukai *An Introduction to Invariants and Moduli*
82 G. Tourlakis *Lectures in Logic and Set Theory, I*
83 G. Tourlakis *Lectures in Logic and Set Theory, II*
84 R. A. Bailey *Association Schemes*
85 J. Carlson, S. Müller-Stach & C. Peters *Period Mappings and Period Domains*
86 J. J. Duistermaat & J. A. C. Kolk *Multidimensional Real Analysis I*
87 J. J. Duistermaat & J. A. C. Kolk *Multidimensional Real Analysis II*
89 M. Golumbic & A. Trenk *Tolerance Graphs*
90 L. Harper *Global Methods for Combinatorial Isoperimetric Problems*
91 I. Moerdijk & J. Mrcun *Introduction to Foliations and Lie Groupoids*
92 J. Kollar, K. E. Smith & A. Corti *Rational and Nearly Rational Varieties*
93 D. Applebaum *Levy Processes and Stochastic Calculus*
94 B. Conrad *Modular Forms and the Ramanujan Conjecture*
95 M. Schechter *An Introduction to Nonlinear Analysis*
96 R. Carter *Lie Algebras of Finite and Affine Type*
97 H. L. Montgomery & R. C Vaughan *Multiplicative Number Theory I*
98 I. Chavel *Riemannian Geometry*
99 D. Goldfeld *Automorphic Forms and L-Functions for the Group GL(n,R)*
100 M. Marcus & J. Rosen *Markov Processes, Gaussian Processes, and Local Times*
101 P. Gille & T. Szamuely *Central Simple Algebras and Galois Cohomology*
102 J. Bertoin *Random Fragmentation and Coagulation Processes*

Multiplicative Number Theory
I. Classical Theory

HUGH L. MONTGOMERY
University of Michigan, Ann Arbor

ROBERT C. VAUGHAN
Pennsylvania State University, University Park

CAMBRIDGE
UNIVERSITY PRESS

CAMBRIDGE UNIVERSITY PRESS
Cambridge, New York, Melbourne, Madrid, Cape Town,
Singapore, São Paulo, Delhi, Tokyo, Mexico City

Cambridge University Press
The Edinburgh Building, Cambridge CB2 8RU, UK

Published in the United States of America by Cambridge University Press, New York

www.cambridge.org
Information on this title: www.cambridge.org/9780521849036

First published 2007

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

ISBN 978-0-521-84903-6 Hardback

Dedicated to our teachers:

P. T. Bateman
J. H. H. Chalk
H. Davenport
T. Estermann
H. Halberstam
A. E. Ingham

Talet är tänkandets början och slut.
Med tanken föddes talet.
Utöfver talet når tanken icke.

Numbers are the beginning and end of thinking.
With thoughts were numbers born.
Beyond numbers thought does not reach.

MAGNUS GUSTAF MITTAG-LEFFLER, 1903

Contents

Preface

Our object is to introduce the interested student to the techniques, results, and terminology of multiplicative number theory. It is not intended that our discussion will always reach the research frontier. Rather, it is hoped that the material here will prepare the student for intelligent reading of the more advanced research literature.

Analytic number theorists are not very uniformly distributed around the world and it possible that a student may be working without the guidance of an experienced mentor in the area. With this in mind, we have tried to make this volume as self-contained as possible.

We assume that the reader has some acquaintance with the fundamentals of elementary number theory, abstract algebra, measure theory, complex analysis, and classical harmonic analysis. More specialized or advanced background material in analysis is provided in the appendices.

The relationship of exercises to the material developed in a given section varies widely. Some exercises are designed to illustrate the theory directly whilst others are intended to give some idea of the ways in which the theory can be extended, or developed, or paralleled in other areas. The reader is cautioned that papers cited in exercises do not necessarily contain a solution.

This volume is the first instalment of a larger project. We are preparing a second volume, which will cover such topics as uniform distribution, bounds for exponential sums, a wider zero-free region for the Riemann zeta function, mean and large values of Dirichlet polynomials, approximate functional equations, moments of the zeta function and L functions on the line $\sigma = 1/2$, the large sieve, Vinogradov's method of prime number sums, zero density estimates, primes in arithmetic progressions on average, sums of primes, sieve methods, the distribution of additive functions and mean values of multiplicative functions, and the least prime in an arithmetic progression. The present volume was twenty-five years in preparation—we hope to be a little quicker with the second volume.

Many people have assisted us in this work—including P. T. Bateman, E. Bombieri, T. Chan, J. B. Conrey, H. G. Diamond, T. Estermann, J. B. Friedlander, S. W. Graham, S. M. Gonek, A. Granville, D. R. Heath-Brown, H. Iwaniec, H. Maier, G. G. Martin, D. W. Masser, A. M. Odlyzko, G. Peng, C. Pomerance, H.–E. Richert, K. Soundararajan, and U. M. A. Vorhauer. In particular, our doctoral students, and their students also, have been most helpful in detecting errors of all types. We are grateful to them all. We would be most happy to hear from any reader who detects a misprint, or might suggest improvements.

Finally we thank our loved ones and friends for their long term support and the long–suffering David Tranah at Cambridge University Press for his forbearance.

Notation

Symbol	Meaning	Found on page
$\mathbb{C}$	The set of complex numbers.	109
$\mathbb{F}_p$	A field of p elements.	9
$\mathbb{N}$	The set of natural numbers, 1, 2, ...	114
$\mathbb{Q}$	The set of rational numbers.	120
$\mathbb{R}$	The set of real numbers.	43
$\mathbb{T}$	$\mathbb{R}/\mathbb{Z}$, known as the *circle group* or the *one-dimensional torus*, which is to say the real numbers modulo 1.	110
$\mathbb{Z}$	The set of rational integers.	20
B	constant in the Hadamard product for $\xi(s)$	347, 349
B_k	Bernoulli numbers.	496ff
$B_k(x)$	Bernoulli polynomials.	45, 495ff
$B(\chi)$	constant in the Hadamard product for $\xi(s, \chi)$	351, 352
C_0	Euler's constant	26
$c_q(n)$	The sum of $e(an/q)$ with a running over a reduced residue system modulo q; known as *Ramanujan's sum*.	110
$c_\chi(n)$	$= \sum_{a=1}^{q} \chi(a)e(an/q)$.	286, 290
$d(n)$	The number of positive divisors of n, called the *divisor function*.	2
$d_k(n)$	The number of ordered k-tuples of positive integers whose product is n.	43
$E_0(\chi)$	$= 1$ if $\chi = \chi_0$, 0 otherwise.	358

Symbol	Meaning	Found on page
E_k	The *Euler numbers*, also known as the *secant coefficients*.	506
$e(\theta)$	$= e^{2\pi i\theta}$; the complex exponential with period 1.	64, 108ff
$L(s,\chi)$	A Dirichlet L-function.	120
$\mathrm{Li}(x)$	$= \int_0^x \frac{du}{\log u}$ with the Cauchy principal value taken at 1; the *logarithmic integral*.	189
$\mathrm{li}(x)$	$= \int_2^x \frac{du}{\log u}$; the *logarithmic integral*.	5
$M(x)$	$= \sum_{n\le x} \mu(n)$	182
$M(x;q,a)$	The sum of $\mu(n)$ over those $n \le x$ for which $n \equiv a \pmod q$.	383
$M(x,\chi)$	The sum of $\chi(n)\mu(n)$ over those $n \le x$.	383
$N(T)$	The number of zeros $\rho = \beta + i\gamma$ of $\zeta(s)$ with $0 < \gamma \le T$.	348, 452ff
$N(T,\chi)$	The number of zeros $\rho = \beta + i\gamma$ of $L(s,\chi)$ with $\beta > 0$ and $0 \le \beta \le T$.	454
$P(n)$	The largest prime factor of n.	202
$Q(x)$	the number of square-free numbers not exceeding x	36
$S(t)$	$= \frac{1}{\pi} \arg\zeta(\frac{1}{2} + it)$.	452
$S(t,\chi)$	$= \frac{1}{\pi} \arg L(\frac{1}{2} + it, \chi)$.	454
$\mathrm{si}(x)$	$= -\int_x^\infty \frac{\sin u}{u}\,du$; the *sine integral*.	139
T_k	The *tangent coefficients*.	505
$w(u)$	The *Buchstab function*, defined by the equation $(uw(u))' = w(u-1)$ for $u > 2$ together with the initial condition $w(u) = 1/u$ for $1 < u \le 2$.	216
$Z(t)$	Hardy's function. The function $Z(t)$ is real-valued, and $\lvert Z(t)\rvert = \lvert\zeta(\frac{1}{2} + it)\rvert$.	456ff
β	The real part of a zero of the zeta function or of an L-function.	173
$\Gamma(s)$	$= \int_0^\infty e^{-x} x^{s-1}\,dx$ for $\sigma > 0$; called the *Gamma function*.	30, 520ff

Symbol	Meaning	Found on page
$\Gamma(s, a)$	$= \int_a^\infty e^{-w} w^{s-1}\, dw$; the *incomplete Gamma function*.	327
γ	The imaginary part of a zero of the zeta function or of an L-function.	172
$\Delta_N(\theta)$	$= 1 + 2\sum_{n=1}^{N-1}(1 - n/N)\cos 2\pi n\theta$; known as the *Fejér kernel*.	174
$\varepsilon(\chi)$	$= \tau(\chi)/\big(i^\kappa q^{1/2}\big)$.	332
$\zeta(s)$	$= \sum_{n=1}^\infty n^{-s}$ for $\sigma > 1$, known as *the Riemann zeta function*.	2
$\zeta(s, \alpha)$	$= \sum_{n=0}^\infty (n + \alpha)^{-s}$ for $\sigma > 1$; known as the *Hurwitz zeta function*.	30
$\zeta_K(s)$	$\sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$; known as the *Dedekind zeta function* of the algebraic number field K.	343
Θ	$= \sup \Re \rho$	430, 463
$\vartheta(x)$	$= \sum_{p \le x} \log p$.	46
$\vartheta(z)$	$= \sum_{n=-\infty}^\infty e^{-\pi n^2 z}$ for $\Re z > 0$.	329
$\vartheta(x; q, a)$	The sum of $\log p$ over primes $p \le x$ for which $p \equiv a \pmod q$.	128, 377ff
$\vartheta(x, \chi)$	$= \sum_{p \le x} \chi(p) \log p$.	377ff
κ	$= (1 - \chi(-1))/2$.	332
$\Lambda(n)$	$= \log p$ if $n = p^k$, $= 0$ otherwise; known as the *von Mangoldt Lambda function*.	23
$\Lambda_2(n)$	$= \Lambda(n) \log n + \sum_{bc=n} \Lambda(b)\Lambda(c)$.	251
$\Lambda(x; q, a)$	The sum of $\lambda(n)$ over those $n \le x$ such that $n \equiv a \pmod q$.	383
$\Lambda(x, \chi)$	$= \sum_{n \le x} \chi(n)\lambda(n)$.	383
$\lambda(n)$	$= (-1)^{\Omega(n)}$; known as the *Liouville lambda function*.	21
$\mu(n)$	$= (-1)^{\omega(n)}$ for square-free n, $= 0$ otherwise. Known as the *Möbius mu function*.	21
$\mu(\sigma)$	the Lindelöf mu function	330
$\xi(s)$	$= \frac{1}{2}s(s - 1)\zeta(s)\Gamma(s/2)\pi^{-s/2}$.	328
$\xi(s, \chi)$	$= L(s, \chi)\Gamma((s + \kappa)/2)(q/\pi)^{(s+\kappa)/2}$ where χ is a primitive character modulo q, $q > 1$.	333

Symbol	Meaning	Found on page
$\Pi(x)$	$= \sum_{n\le x} \Lambda(n)/\log n$.	416
$\pi(x)$	The number of primes not exceeding x.	3
$\pi(x;q,a)$	The number of $p \le x$ such that $p \equiv a \pmod q$,.	90, 358
$\pi(x,\chi)$	$= \sum_{p\le x} \chi(p)$.	377ff
ρ	$= \beta + i\gamma$; a zero of the zeta function or of an L-function.	173
$\rho(u)$	The *Dickman function*, defined by the equation $u\rho'(u) = -\rho(u-1)$ for $u > 1$ together with the initial condition $\rho(u) = 1$ for $0 \le u \le 1$.	200
$\sigma(n)$	The sum of the positive divisors of n.	27
$\sigma_a(n)$	$= \sum_{d\mid n} d^a$.	28
τ	$= \lvert t\rvert + 4$.	14
$\tau(\chi)$	$= \sum_{a=1}^{q} \chi(a)e(a/q)$; known as the *Gauss sum* of χ.	286ff
$\Phi_q(z)$	The q^{th} cyclotomic polynomial, which is to say a monic polynomial with integral coefficients, of degree $\varphi(q)$, whose roots are the numbers $e(a/q)$ for $(a,q) = 1$.	64
$\Phi(x,y)$	The number of $n \le x$ such that all prime factors of n are $\ge y$.	215
$\Phi(y)$	$= \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y} e^{-t^2/2}\,dt$; the cumulative distribution function of a normal random variable with mean 0 and variance 1.	235
$\varphi(n)$	The number of a, $1 \le a \le n$, for which $(a,n) = 1$; known as *Euler's totient function*.	27
$\chi(n)$	A Dirichlet character.	115
$\psi(x)$	$= \sum_{n\le x} \Lambda(n)$.	46
$\psi(x,y)$	The number of $n \le x$ composed entirely of primes $p \le y$.	199
$\psi(x;q,a)$	The sum of $\Lambda(n)$ over $n \le x$ for which $n \equiv a \pmod q$.	128, 377ff
$\psi(x,\chi)$	$= \sum_{n\le x} \chi(n)\Lambda(n)$.	377ff
$\Omega(n)$	The number of prime factors of n, counting multiplicity.	21
$\omega(n)$	The number of distinct primes dividing n.	21

Symbol	Meaning	Found on page
$[x]$	The unique integer such that $[x] \le x < [x] + 1$; called the *integer part* of x.	15, 24
$\{x\}$	$= x - [x]$; called the *fractional part* of x.	24
$\|x\|$	The distance from x to the nearest integer.	477
$f(x) = O(g(x))$	$\lvert f(x)\rvert \le Cg(x)$ where C is an absolute constant.	3
$f(x) = o(g(x))$	$\lim f(x)/g(x) = 0$.	3
$f(x) \ll g(x)$	$f(x) = O(g(x))$.	3
$f(x) \gg g(x)$	$g(x) = O(f(x))$, g non-negative.	4
$f(x) \asymp g(x)$	$cf(x) \le g(x) \le Cf(x)$ for some positive absolute constants c, C.	4
$f(x) \sim g(x)$	$\lim f(x)/g(x) = 1$.	3