Graduate Texts in Mathematics

74

Multiplicative Number Theory

Springer-Verlag

Harold Davenport

Multiplicative Number Theory

Third Edition

Springer

Harold Davenport
(Deceased)

Hugh L. Montgomery
Department of Mathematics
University of Michigan
Ann Arbor, MI 48109-1109
USA
hlm@math.lsa.umich.edu

Mathematics Subject Classification (2000): 11-01, 11Nxx

Library of Congress Cataloging-in-Publication Data
Davenport, Harold, 1907-
Multiplicative number theory / Harold Davenport. – 3rd ed. / revised by Hugh L. Montgomery.
p. cm. – (Graduate texts in mathematics; 74)
Includes bibliographical references and index.
ISBN 0-387-95097-4 (soft:alk. paper)
1. Number theory. 2. Numbers, Prime. I. Montgomery, Hugh L. II. Title. III. Series.
QA241 .D32 2000
512'.74—dc21 00-056313

Printed on acid-free paper.

The first edition of this book was published by Markham Publishing Company, Chicago, IL, 1967.

Production managed by Yong-Soon Hwang; manufacturing supervised by Erica Bresler.
Printed and bound by Sheridan Books, Inc., Ann Arbor, MI.
Printed in the United States of America.

9 8 7 6 5 4 3 2 1

ISBN 0-387-95097-4 SPIN 10773281

Springer-Verlag New York Berlin Heidelberg
A member of BertelsmannSpringer Science+Business Media GmbH

Graduate Texts in Mathematics 74

Springer
New York
Berlin
Heidelberg
Barcelona
Hong Kong
London
Milan
Paris
Singapore
Tokyo

Graduate Texts in Mathematics

1 TAKEUTI/ZARING. Introduction to Axiomatic Set Theory. 2nd ed.
2 OXTOBY. Measure and Category. 2nd ed.
3 SCHAEFER. Topological Vector Spaces. 2nd ed.
4 HILTON/STAMMBACH. A Course in Homological Algebra. 2nd ed.
5 MAC LANE. Categories for the Working Mathematician. 2nd ed.
6 HUGHES/PIPER. Projective Planes.
7 SERRE. A Course in Arithmetic.
8 TAKEUTI/ZARING. Axiomatic Set Theory.
9 HUMPHREYS. Introduction to Lie Algebras and Representation Theory.
0 COHEN. A Course in Simple Homotopy Theory.
1 CONWAY. Functions of One Complex Variable I. 2nd ed.
2 BEALS. Advanced Mathematical Analysis.
3 ANDERSON/FULLER. Rings and Categories of Modules. 2nd ed.
4 GOLUBITSKY/GUILLEMIN. Stable Mappings and Their Singularities.
5 BERBERIAN. Lectures in Functional Analysis and Operator Theory.
6 WINTER. The Structure of Fields.
7 ROSENBLATT. Random Processes. 2nd ed.
8 HALMOS. Measure Theory.
9 HALMOS. A Hilbert Space Problem Book. 2nd ed.
0 HUSEMOLLER. Fibre Bundles. 3rd ed.
1 HUMPHREYS. Linear Algebraic Groups.
2 BARNES/MACK. An Algebraic Introduction to Mathematical Logic.
3 GREUB. Linear Algebra. 4th ed.
4 HOLMES. Geometric Functional Analysis and Its Applications.
5 HEWITT/STROMBERG. Real and Abstract Analysis.
6 MANES. Algebraic Theories.
7 KELLEY. General Topology.
8 ZARISKI/SAMUEL. Commutative Algebra. Vol.I.
9 ZARISKI/SAMUEL. Commutative Algebra. Vol.II.
0 JACOBSON. Lectures in Abstract Algebra I. Basic Concepts.
1 JACOBSON. Lectures in Abstract Algebra II. Linear Algebra.
32 JACOBSON. Lectures in Abstract Algebra III. Theory of Fields and Galois Theory.
33 HIRSCH. Differential Topology.
34 SPITZER. Principles of Random Walk. 2nd ed.
35 ALEXANDER/WERMER. Several Complex Variables and Banach Algebras. 3rd ed.
36 KELLEY/NAMIOKA et al. Linear Topological Spaces.
37 MONK. Mathematical Logic.
38 GRAUERT/FRITZSCHE. Several Complex Variables.
39 ARVESON. An Invitation to C^*-Algebras.
40 KEMENY/SNELL/KNAPP. Denumerable Markov Chains. 2nd ed.
41 APOSTOL. Modular Functions and Dirichlet Series in Number Theory. 2nd ed.
42 SERRE. Linear Representations of Finite Groups.
43 GILLMAN/JERISON. Rings of Continuous Functions.
44 KENDIG. Elementary Algebraic Geometry.
45 LOÈVE. Probability Theory I. 4th ed.
46 LOÈVE. Probability Theory II. 4th ed.
47 MOISE. Geometric Topology in Dimensions 2 and 3.
48 SACHS/WU. General Relativity for Mathematicians.
49 GRUENBERG/WEIR. Linear Geometry. 2nd ed.
50 EDWARDS. Fermat's Last Theorem.
51 KLINGENBERG. A Course in Differential Geometry.
52 HARTSHORNE. Algebraic Geometry.
53 MANIN. A Course in Mathematical Logic.
54 GRAVER/WATKINS. Combinatorics with Emphasis on the Theory of Graphs.
55 BROWN/PEARCY. Introduction to Operator Theory I: Elements of Functional Analysis.
56 MASSEY. Algebraic Topology: An Introduction.
57 CROWELL/FOX. Introduction to Knot Theory.
58 KOBLITZ. p-adic Numbers, p-adic Analysis, and Zeta-Functions. 2nd ed.
59 LANG. Cyclotomic Fields.
60 ARNOLD. Mathematical Methods in Classical Mechanics. 2nd ed.

(continued after index)

PREFACE TO THE SECOND AND THIRD EDITIONS

Although it was in print for a short time only, the original edition of *Multiplicative Number Theory* had a major impact on research and on young mathematicians. By giving a connected account of the large sieve and Bombieri's theorem, Professor Davenport made accessible an important body of new discoveries. With this stimulation, such great progress was made that our current understanding of these topics extends well beyond what was known in 1966. As the main results can now be proved much more easily, I made the radical decision to rewrite §§23–29 completely for the second edition. In making these alterations I have tried to preserve the tone and spirit of the original.

Rather than derive Bombieri's theorem from a zero density estimate for L functions, as Davenport did, I have chosen to present Vaughan's elementary proof of Bombieri's theorem. This approach depends on Vaughan's simplified version of Vinogradov's method for estimating sums over prime numbers (see §24). Vinogradov devised his method in order to estimate the sum $\sum_{p\leqslant X} e(p\alpha)$; to maintain the historical perspective I have inserted (in §§25, 26) a discussion of this exponential sum and its application to sums of primes, before turning to the large sieve and Bombieri's theorem.

Before Professor Davenport's untimely death in 1969, several mathematicians had suggested small improvements which might be made in *Multiplicative Number Theory*, should it ever be reprinted. Most of these have been incorporated here; in particular, the nice refinements in §§12 and 14, were suggested by Professor E. Wirsing. Professor L. Schoenfeld detected the only significant error in the book, in the proof of Theorems 4 and 4A of §23. Indeed these theorems are false as they stood, although their corollaries, which were used later, are true. In considering the extent and nature of my revisions, I have benefited from the advice of Professors Baker, Bombieri, Cassels, Halberstam, Hooley, Mack, Schmidt, and Vaughan, although the responsibility for the decisions taken is entirely my own. The assistance throughout of Mrs. H. Davenport and Dr. J. H. Davenport has been invaluable. Finally, the mathematical community is indebted to Professor J.-P. Serre for urging Springer-Verlag to publish a new edition of this important book.

H.L.M.

PREFACE TO THE FIRST EDITION

My principal object in these lectures was to give a connected account of analytic number theory in so far as it relates to problems of a multiplicative character, with particular attention to the distribution of primes in arithmetic progressions. Most of the work is by now classical, and I have followed to a considerable extent the historical order of discovery. I have included some material which, though familiar to experts, cannot easily be found in the existing expositions.

My secondary object was to prove, in the course of this account, all the results quoted from the literature in the recent paper of Bombieri[1] on the average distribution of primes in arithmetic progressions; and to end by giving an exposition of this work, which seems likely to play an important part in future researches. The choice of what was included in the main body of the lectures, and what was omitted, has been greatly influenced by this consideration. A short section has, however, been added, giving some references to other work.

In revising the lectures for publication I have aimed at producing a readable account of the subject, even at the cost of occasionally omitting some details. I hope that it will be found useful as an introduction to other books and monographs on analytic number theory.

§§23 and 29 contain recent joint work of Professor Halberstam and myself, and I am indebted to Professor Halberstam for permission to include this. The former gives our version of the basic principle of the large sieve method, and the latter is an average result on primes in arithmetic progressions which may prove to be

[1] On the large sieve, *Mathematika*, **12**, 201–225 (1965).

a useful supplement to Bombieri's theorem. No account is given of other sieve methods, since these will form the theme of a later volume in this series by Professors Halberstam and Richert.[2]

H.D.

[2] This book subsequently appeared as *Sieve Methods*, Academic Press (London), 1974.

BIBLIOGRAPHY

The following works will be referred to by their authors' names, or by short titles.

Bohr, H., and Cramér, H. *Die neuere Entwicklung der analytischen Zahlentheorie*, Enzyklopädie der mathematischen Wissenschaften, II.3, Heft 6, Teubner, Leipzig, 1923.

Hua, L.-K. *Die Abschätzung von Exponentialsummen und ihre Anwendung in der Zahlentheorie*, Enzyklopädie der mathematischen Wissenschaften, I.2, Heft 13, Teil 1, Teubner, Leipzig, 1959.

Ingham, A. E. *The distribution of prime numbers*, Cambridge Mathematical Tracts No. 30, Cambridge, 1990.

Landau, E. *Handbuch der Lehre von der Verteilung der Primzahlen*, 2nd ed. with an appendix by P. T. Bateman, Chelsea, New York, 1953.

Landau, E. *Vorlesungen über Zahlentheorie*, 3 vol., Hirzel, Leipzig, 1927.

Prachar, K. *Primzahlverteilung*, Springer, Berlin, 1957.

Titchmarsh, E. C. *The theory of the Riemann zeta-function*, Clarendon Press, Oxford, 1986.

NOTATION

We write $f(x) = O(g(x))$, or equivalently $f(x) \ll g(x)$, when there is a constant C such that $|f(x)| \leq Cg(x)$ for all values of x under consideration. We write $f(x) \sim g(x)$ when $\lim f(x)/g(x) = 1$ as x tends to some limit, and $f(x) = o(g(x))$ when $\lim f(x)/g(x) = 0$. Moreover, we say that $f(x) = \Omega(g(x))$ to indicate that $\limsup |f(x)|/g(x) > 0$, while $f(x) = \Omega_{\pm}(g(x))$ means that $\limsup f(x)/g(x) > 0$ and $\liminf f(x)/g(x) < 0$.

If ξ is a vector, then $\|\xi\|$ denotes its norm, while if θ is a real number then $\|\theta\|$ denotes the distance from θ to the nearest integer. In certain contexts (see p. 32), we let $[x]$ denote the largest integer not exceeding the real number x, and we let (x) be the fractional part of x, $(x) = x - [x]$. Generally s denotes a complex variable, $s = \sigma + it$, while $\rho = \beta + i\gamma$ denotes the generic non-trivial zero of the zeta function or of a Dirichlet L function. When no confusion arises, we let γ stand for Euler's constant.

The arithmetic functions $d(n)$, $\Lambda(n)$, $\mu(n)$, and $\phi(n)$ are defined as usual. Other symbols are defined on the following pages.

CONTENTS

1

PRIMES IN ARITHMETIC PROGRESSION

Analytic number theory may be said to begin with the work of Dirichlet, and in particular with Dirichlet's memoir of 1837 on the existence of primes in a given arithmetic progression.

Long before the time of Dirichlet it had been asserted that every arithmetic progression

$$a, a + q, a + 2q, \ldots,$$

in which a and q have no common factor, includes infinitely many primes. Legendre, who had based some of his demonstrations on this proposition, attempted to give a proof but failed. The first proof was that of Dirichlet in the memoir I have referred to (Dirichlet's *Werke*, I, pp. 313–342), and strictly speaking this proof was complete only in the case when q is a prime. For the general case, Dirichlet had to assume his class number formula, which he proved in a paper of 1839–1840 (*Werke*, I, pp. 411–496). Dirichlet states at the end of the earlier paper that originally he had a different proof, by indirect and complicated arguments, of the vital result that was needed [the fact that $L(1, \chi) \neq 0$ for each real nonprincipal character χ; see §4], but I do not think that there is any indication anywhere of its nature.

I shall follow Dirichlet's example in treating first the simpler case in which q is a prime. We can suppose that $q > 2$, for when $q = 2$ the arithmetic progression contains all sufficiently large odd numbers, and the proposition is then a triviality.

Dirichlet's starting point, as he himself says, was Euler's proof of the existence of infinitely many primes. If we write

$$\zeta(s) = \sum_{n=1}^{\infty} n^{-s},$$

for a real variable $s > 1$, then Euler's identity is

$$\zeta(s) = \prod_{p} (1 - p^{-s})^{-1}$$

for $s > 1$, where p runs through all the primes; this identity is an analytic equivalent for the proposition that every natural number can be factorized into prime powers in one and only one way. It follows from the identity that

$$\log \zeta(s) = \sum_p \sum_{m=1}^{\infty} m^{-1} p^{-ms}.$$

Since $\zeta(s) \to \infty$ as $s \to 1$ from the right, and since

$$\sum_p \sum_{m=2}^{\infty} m^{-1} p^{-ms} < \sum_p \sum_{m=2}^{\infty} p^{-m} = \sum_p \frac{1}{p(p-1)} < 1,$$

it follows that

$$\sum_p p^{-s} \to \infty$$

as $s \to 1$ from the right. This proves the existence of an infinity of primes, and proves further that the series Σp^{-1}, extended over the primes, diverges. Dirichlet's aim was to prove the analogous statements when the primes p are limited to those which satisfy the condition $p \equiv a \pmod q$.

To this end he introduced the arithmetic functions called Dirichlet's characters. Each of these is a function of the integer variable n, which is periodic with period q and is also multiplicative (without any restriction). Moreover, these functions are such that a suitable linear combination of them will produce the function which is 1 if $n \equiv a \pmod q$ and 0 otherwise.

The construction of these functions is based on the existence of a primitive root to the (prime) modulus q, or in other words on the cyclic structure of the residue classes modulo q under multiplication, when 0 is excluded. Let $\nu(n)$ denote the index of n relative to a fixed primitive root g, that is, the exponent ν for which $g^\nu \equiv n$. Let ω be a real or complex number satisfying

$$\omega^{q-1} = 1.$$

Then the typical Dirichlet character for the modulus q is

$$\omega^{\nu(n)},$$

which is uniquely defined, since the value of $\nu(n)$ is indeterminate only to the extent of the addition of a multiple of $q - 1$. The definition presupposes that n is not divisible by q, but it is convenient to complete the definition by taking the function to be 0 when n is divisible by q. There is one function for each choice of ω, and different choices of ω give different functions; thus there are $q - 1$ such functions. Each is a periodic function of n with period q, and is multiplicative because, if

$$n \equiv n_1 n_2 \pmod{q},$$

then

$$\nu(n) \equiv \nu(n_1) + \nu(n_2) \pmod{q-1}.$$

(We have supposed here that neither n_1 nor n_2 is divisible by q, but the multiplicative property is a triviality if either of them is.)

We recall the well-known fact that $\Sigma_\omega \omega^k$ has the value $q - 1$ if k is divisible by $q - 1$ and has the value 0 otherwise. Hence

$$\sum_\omega \omega^{-\nu(a)}\omega^{\nu(n)} = \begin{cases} q-1 & \text{if } n \equiv a \pmod{q}, \\ 0 & \text{otherwise,} \end{cases}$$

since $\nu(n) \equiv \nu(a) \pmod{q-1}$ if and only if $n \equiv a \pmod{q}$. The expression on the left, after division by $q - 1$, is the linear combination of the various functions $\omega(n)$ that was referred to above; it serves to select from all integers n those that are congruent to the given number a to the modulus q.

For each of the possible choices for ω, Dirichlet introduced the function

$$L_\omega(s) = \sum_{\substack{n=1 \\ n \not\equiv 0 \pmod{q}}}^{\infty} \omega^{\nu(n)} n^{-s}$$

of the real variable s, for $s > 1$. Since the coefficient of n^{-s} is a multiplicative function of n, we have the analog of Euler's identity:

$$L_\omega(s) = \prod_{p \neq q} (1 - \omega^{\nu(p)} p^{-s})^{-1},$$

for $s > 1$. A detailed proof is easily given, on the same lines as for Euler's original identity, by considering first the finite product over $p \leq N$ and then making $N \to \infty$.

None of the factors on the right vanishes, since $|\omega^{\nu(p)}p^{-s}| = p^{-s} < \frac{1}{2}$ for $s > 1$, and as the product is absolutely convergent it follows that $L_\omega(s) \neq 0$ for $s > 1$. Taking the logarithm of both sides, we get

$$\log L_\omega(s) = \sum_{p \neq q} \sum_{m=1}^{\infty} m^{-1} \omega^{\nu(p^m)} p^{-ms}.$$

The logarithm on the left is, in principle, multivalued if ω is complex, but the value which is provided by the series on the right is obviously the natural one to use, since it is a continuous function of s for $s > 1$ and tends to 0 as $s \to \infty$, corresponding to the fact that $L_\omega(s) \to 1$ (1 being the first term in its defining series).

Multiplying the last equation by $\omega^{-\nu(a)}$ and summing over all the values of ω, we obtain

$$(1) \qquad \frac{1}{q-1}\sum_{\omega} \omega^{-\nu(a)} \log L_\omega(s) = \sum_{\substack{p \\ p^m \equiv a \pmod q}} \sum_{m=1}^{\infty} m^{-1}p^{-ms}.$$

The sum of all those terms on the right for which $m > 1$ is at most 1, since they are a subset of the terms considered earlier in connection with $\log \zeta(s)$. Hence the right side of (1) is

$$\sum_{p \equiv a \pmod q} p^{-s} + O(1).$$

The essential idea of Dirichlet's memoir is to prove that the left side of (1) tends to $+\infty$ as $s \to 1$. This will imply that there are infinitely many primes $p \equiv a \pmod q$, and further that the series Σp^{-1} extended over these primes is divergent.

One of the terms in the sum on the left of (1) comes from $\omega = 1$, and is simply $\log L_1(s)$. The function $L_1(s)$ is related in a simple way to $\zeta(s)$, for we have

$$L_1(s) = \sum_{\substack{n=1 \\ q \nmid n}}^{\infty} n^{-s} = (1 - q^{-s})\zeta(s).$$

Hence $L_1(s) \to +\infty$ as $s \to 1$ from the right, and therefore the same is true of $\log L_1(s)$. Hence to complete the proof it will suffice to show that, for each choice of ω other than 1,

$$\log L_\omega(s)$$

is bounded as $s \to 1$ from the right.

At this point it clarifies the situation if we observe that, provided $\omega \neq 1$, the series which defines $L_\omega(s)$, namely

$$L_\omega(s) = \sum_{\substack{n=1 \\ n \not\equiv 0 \pmod q}}^{\infty} \omega^{\nu(n)} n^{-s},$$

is convergent not only for $s > 1$ but for $s > 0$. It is, in fact, a series of the type covered by Dirichlet's test for convergence, since (a) n^{-s} decreases as n increases and has the limit 0, and (b) the sum of any number of the coefficients $\omega^{\nu(n)}$ is bounded. The justification for (b) lies in the fact that $\omega^{\nu(n)}$ is periodic with period q, and

$$\sum_{n=1}^{q-1} \omega^{\nu(n)} = \sum_{m=0}^{q-2} \omega^m = 0,$$

since the index $\nu(n)$ runs through a complete set of residues to the modulus $q - 1$.

It follows further from Dirichlet's test that the series is uniformly convergent with respect to s for $s \geq \delta > 0$, and consequently $L_\omega(s)$ is a continuous function of s for $s > 0$. So to prove that $\log L_\omega(s)$ is bounded as $s \to 1$ from the right is equivalent to proving that

$$L_\omega(1) \neq 0. \tag{2}$$

Dirichlet's proof of this takes entirely different forms according as ω is real or complex. The only real value of ω is -1, since $\omega \neq 1$ now.

Suppose first that ω is complex. If we take $a = 1$, and so $\nu(a) = 0$, in (1), we get

$$\frac{1}{q-1}\sum_\omega \log L_\omega(s) = \sum_{p}\sum_{\substack{m=1 \\ p^m \equiv 1 \pmod q}}^{\infty} m^{-1}p^{-ms}.$$

Since the terms on the right (if there are any) are positive, it follows that

$$\sum_\omega \log L_\omega(s) \geq 0,$$

which implies that

$$\prod_\omega L_\omega(s) \geq 1. \tag{3}$$

All this, of course, is for $s > 1$.

If there is some complex ω for which $L_\omega(1) = 0$, then $L_{\bar\omega}(1) = 0$ also, where $\bar\omega$ denotes the complex conjugate of ω. Thus two of the factors on the left of (3) will have the limit 0 as $s \to 1$ from the right. One other factor, namely $L_1(s)$, has the limit $+\infty$. Any other factors are certainly bounded, being continuous functions of s for $s > 0$. On examining in more detail the behavior as $s \to 1$ of the three factors mentioned, we shall get a contradiction to (3), in that the two factors with limit 0 will more than cancel the one factor with limit $+\infty$.

As regards $L_1(s)$, we have

$$L_1(s) = (1 - q^{-s})\zeta(s) < (1 - q^{-2})\zeta(s)$$