PURE AND APPLIED MATHEMATICS

*A Series of Monographs and Textbooks*

# NUMBER THEORY ARISING FROM FINITE FIELDS

## Analytic and Probabilistic Theory

John Knopfmacher
Wen-Bin Zhang

# NUMBER THEORY ARISING FROM FINITE FIELDS

# NUMBER THEORY ARISING FROM FINITE FIELDS

## Analytic and Probabilistic Theory

John Knopfmacher

*University of the Witwatersrand*
*Johannesburg, South Africa*

Wen-Bin Zhang

*University of the West Indies*
*Kingston, Jamaica*

MARCEL DEKKER

MARCEL DEKKER, INC.    NEW YORK • BASEL

**ISBN: 0-8247-0577-7**

This book is printed on acid-free paper.

**Headquarters**
Marcel Dekker, Inc.
270 Madison Avenue, New York, NY 10016
tel: 212-696-9000; fax: 212-685-4540

**Eastern Hemisphere Distribution**
Marcel Dekker AG
Hutgasse 4, Postfach 812, CH-4001 Basel, Switzerland
tel: 41-61-261-8482; fax: 41-61-261-8896

**World Wide Web**
http://www.dekker.com

The publisher offers discounts on this book when ordered in bulk quantities. For more information, write to Special Sales/Professional Marketing at the headquarters address above.

Current printing (last digit):
10 9 8 7 6 5 4 3 2 1

**PRINTED IN THE UNITED STATES OF AMERICA**

# PURE AND APPLIED MATHEMATICS

## A Program of Monographs, Textbooks, and Lecture Notes

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

# MONOGRAPHS AND TEXTBOOKS IN PURE AND APPLIED MATHEMATICS

1. *K. Yano,* Integral Formulas in Riemannian Geometry (1970)
2. *S. Kobayashi,* Hyperbolic Manifolds and Holomorphic Mappings (1970)
3. *V. S. Vladimirov,* Equations of Mathematical Physics (A. Jeffrey, ed.; A. Littlewood, trans.) (1970)
4. *B. N. Pshenichnyi,* Necessary Conditions for an Extremum (L. Neustadt, translation ed.; K. Makowski, trans.) (1971)
5. *L. Narici et al.,* Functional Analysis and Valuation Theory (1971)
6. *S. S. Passman,* Infinite Group Rings (1971)
7. *L. Dornhoff,* Group Representation Theory. Part A: Ordinary Representation Theory. Part B: Modular Representation Theory (1971, 1972)
8. *W. Boothby and G. L. Weiss, eds.,* Symmetric Spaces (1972)
9. *Y. Matsushima,* Differentiable Manifolds (E. T. Kobayashi, trans.) (1972)
10. *L. E. Ward, Jr.,* Topology (1972)
11. *A. Babakhanian,* Cohomological Methods in Group Theory (1972)
12. *R. Gilmer,* Multiplicative Ideal Theory (1972)
13. *J. Yeh,* Stochastic Processes and the Wiener Integral (1973)
14. *J. Barros-Neto,* Introduction to the Theory of Distributions (1973)
15. *R. Larsen,* Functional Analysis (1973)
16. *K. Yano and S. Ishihara,* Tangent and Cotangent Bundles (1973)
17. *C. Procesi,* Rings with Polynomial Identities (1973)
18. *R. Hermann,* Geometry, Physics, and Systems (1973)
19. *N. R. Wallach,* Harmonic Analysis on Homogeneous Spaces (1973)
20. *J. Dieudonné,* Introduction to the Theory of Formal Groups (1973)
21. *I. Vaisman,* Cohomology and Differential Forms (1973)
22. *B.-Y. Chen,* Geometry of Submanifolds (1973)
23. *M. Marcus,* Finite Dimensional Multilinear Algebra (in two parts) (1973, 1975)
24. *R. Larsen,* Banach Algebras (1973)
25. *R. O. Kujala and A. L. Vitter, eds.,* Value Distribution Theory: Part A; Part B: Deficit and Bezout Estimates by Wilhelm Stoll (1973)
26. *K. B. Stolarsky,* Algebraic Numbers and Diophantine Approximation (1974)
27. *A. R. Magid,* The Separable Galois Theory of Commutative Rings (1974)
28. *B. R. McDonald,* Finite Rings with Identity (1974)
29. *J. Satake,* Linear Algebra (S. Koh et al., trans.) (1975)
30. *J. S. Golan,* Localization of Noncommutative Rings (1975)
31. *G. Klambauer,* Mathematical Analysis (1975)
32. *M. K. Agoston,* Algebraic Topology (1976)
33. *K. R. Goodearl,* Ring Theory (1976)
34. *L. E. Mansfield,* Linear Algebra with Geometric Applications (1976)
35. *N. J. Pullman,* Matrix Theory and Its Applications (1976)
36. *B. R. McDonald,* Geometric Algebra Over Local Rings (1976)
37. *C. W. Groetsch,* Generalized Inverses of Linear Operators (1977)
38. *J. E. Kuczkowski and J. L. Gersting,* Abstract Algebra (1977)
39. *C. O. Christenson and W. L. Voxman,* Aspects of Topology (1977)
40. *M. Nagata,* Field Theory (1977)
41. *R. L. Long,* Algebraic Number Theory (1977)
42. *W. F. Pfeffer,* Integrals and Measures (1977)
43. *R. L. Wheeden and A. Zygmund,* Measure and Integral (1977)
44. *J. H. Curtiss,* Introduction to Functions of a Complex Variable (1978)
45. *K. Hrbacek and T. Jech,* Introduction to Set Theory (1978)
46. *W. S. Massey,* Homology and Cohomology Theory (1978)
47. *M. Marcus,* Introduction to Modern Algebra (1978)
48. *E. C. Young,* Vector and Tensor Analysis (1978)
49. *S. B. Nadler, Jr.,* Hyperspaces of Sets (1978)
50. *S. K. Segal,* Topics in Group Kings (1978)
51. *A. C. M. van Rooij,* Non-Archimedean Functional Analysis (1978)
52. *L. Corwin and R. Szczarba,* Calculus in Vector Spaces (1979)
53. *C. Sadosky,* Interpolation of Operators and Singular Integrals (1979)
54. *J. Cronin,* Differential Equations (1980)
55. *C. W. Groetsch,* Elements of Applicable Functional Analysis (1980)

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

56. *I. Vaisman,* Foundations of Three-Dimensional Euclidean Geometry (1980)
57. *H. I. Freedan,* Deterministic Mathematical Models in Population Ecology (1980)
58. *S. B. Chae,* Lebesgue Integration (1980)
59. *C. S. Rees et al.,* Theory and Applications of Fourier Analysis (1981)
60. *L. Nachbin,* Introduction to Functional Analysis (R. M. Aron, trans.) (1981)
61. *G. Orzech and M. Orzech,* Plane Algebraic Curves (1981)
62. *R. Johnsonbaugh and W. E. Pfaffenberger,* Foundations of Mathematical Analysis (1981)
63. *W. L. Voxman and R. H. Goetschel,* Advanced Calculus (1981)
64. *L. J. Corwin and R. H. Szczarba,* Multivariable Calculus (1982)
65. *V. I. Istrățescu,* Introduction to Linear Operator Theory (1981)
66. *R. D. Järvinen,* Finite and Infinite Dimensional Linear Spaces (1981)
67. *J. K. Beem and P. E. Ehrlich,* Global Lorentzian Geometry (1981)
68. *D. L. Armacost,* The Structure of Locally Compact Abelian Groups (1981)
69. *J. W. Brewer and M. K. Smith, eds.,* Emmy Noether: A Tribute (1981)
70. *K. H. Kim,* Boolean Matrix Theory and Applications (1982)
71. *T. W. Wieting,* The Mathematical Theory of Chromatic Plane Ornaments (1982)
72. *D. B.Gauld,* Differential Topology (1982)
73. *R. L. Faber,* Foundations of Euclidean and Non-Euclidean Geometry (1983)
74. *M. Carmeli,* Statistical Theory and Random Matrices (1983)
75. *J. H. Carruth et al.,* The Theory of Topological Semigroups (1983)
76. *R. L. Faber,* Differential Geometry and Relativity Theory (1983)
77. *S. Barnett,* Polynomials and Linear Control Systems (1983)
78. *G. Karpilovsky,* Commutative Group Algebras (1983)
79. *F. Van Oystaeyen and A. Verschoren,* Relative Invariants of Rings (1983)
80. *I. Vaisman,* A First Course in Differential Geometry (1984)
81. *G. W. Swan,* Applications of Optimal Control Theory in Biomedicine (1984)
82. *T. Petrie and J. D. Randall, Transformation Groups on Manifolds (1984)*
83. *K. Goebel and S. Reich,* Uniform Convexity, Hyperbolic Geometry, and Nonexpansive Mappings (1984)
84. *T. Albu and C. Năstăsescu,* Relative Finiteness in Module Theory (1984)
85. *K. Hrbacek and T. Jech,* Introduction to Set Theory: Second Edition (1984)
86. *F. Van Oystaeyen and A. Verschoren,* Relative Invariants of Rings (1984)
87. *B. R. McDonald,* Linear Algebra Over Commutative Rings (1984)
88. *M. Namba,* Geometry of Projective Algebraic Curves (1984)
89. *G. F. Webb,* Theory of Nonlinear Age-Dependent Population Dynamics (1985)
90. *M. R. Bremner et al.,* Tables of Dominant Weight Multiplicities for Representations of Simple Lie Algebras (1985)
91. *A. E. Fekete,* Real Linear Algebra (1985)
92. *S. B. Chae,* Holomorphy and Calculus in Normed Spaces (1985)
93. *A. J. Jerri,* Introduction to Integral Equations with Applications (1985)
94. *G. Karpilovsky,* Projective Representations of Finite Groups (1985)
95. *L. Narici and E. Beckenstein,* Topological Vector Spaces (1985)
96. *J. Weeks,* The Shape of Space (1985)
97. *P. R. Gribik and K. O. Kortanek,* Extremal Methods of Operations Research (1985)
98. *J.-A. Chao and W. A. Woyczynski, eds.,* Probability Theory and Harmonic Analysis (1986)
99. *G. D. Crown et al.,* Abstract Algebra (1986)
100. *J. H. Carruth et al.,* The Theory of Topological Semigroups, Volume 2 (1986)
101. *R. S. Doran and V. A. Belfi,* Characterizations of C*-Algebras (1986)
102. *M. W. Jeter,* Mathematical Programming (1986)
103. *M. Altman,* A Unified Theory of Nonlinear Operator and Evolution Equations with Applications (1986)
104. *A. Verschoren,* Relative Invariants of Sheaves (1987)
105. *R. A. Usmani,* Applied Linear Algebra (1987)
106. *P. Blass and J. Lang,* Zariski Surfaces and Differential Equations in Characteristic $p > 0$ (1987)
107. *J. A. Reneke et al.,* Structured Hereditary Systems (1987)
108. *H. Busemann and B. B. Phadke,* Spaces with Distinguished Geodesics (1987)
109. *R. Harte,* Invertibility and Singularity for Bounded Linear Operators (1988)
110. *G. S. Ladde et al.,* Oscillation Theory of Differential Equations with Deviating Arguments (1987)
111. *L. Dudkin et al.,* Iterative Aggregation Theory (1987)
112. *T. Okubo,* Differential Geometry (1987)

113. *D. L. Stancl and M. L. Stancl,* Real Analysis with Point-Set Topology (1987)
114. *T. C. Gard,* Introduction to Stochastic Differential Equations (1988)
115. *S. S. Abhyankar,* Enumerative Combinatorics of Young Tableaux (1988)
116. *H. Strade and R. Farnsteiner,* Modular Lie Algebras and Their Representations (1988)
117. *J. A. Huckaba,* Commutative Rings with Zero Divisors (1988)
118. *W. D. Wallis,* Combinatorial Designs (1988)
119. *W. Więsław,* Topological Fields (1988)
120. *G. Karpilovsky,* Field Theory (1988)
121. *S. Caenepeel and F. Van Oystaeyen,* Brauer Groups and the Cohomology of Graded Rings (1989)
122. *W. Kozlowski,* Modular Function Spaces (1988)
123. *E. Lowen-Colebunders,* Function Classes of Cauchy Continuous Maps (1989)
124. *M. Pavel,* Fundamentals of Pattern Recognition (1989)
125. *V. Lakshmikantham et al.,* Stability Analysis of Nonlinear Systems (1989)
126. *R. Sivaramakrishnan,* The Classical Theory of Arithmetic Functions (1989)
127. *N. A. Watson,* Parabolic Equations on an Infinite Strip (1989)
128. *K. J. Hastings,* Introduction to the Mathematics of Operations Research (1989)
129. *B. Fine,* Algebraic Theory of the Bianchi Groups (1989)
130. *D. N. Dikranjan et al.,* Topological Groups (1989)
131. *J. C. Morgan II,* Point Set Theory (1990)
132. *P. Biler and A. Witkowski,* Problems in Mathematical Analysis (1990)
133. *H. J. Sussmann,* Nonlinear Controllability and Optimal Control (1990)
134. *J.-P. Florens et al.,* Elements of Bayesian Statistics (1990)
135. *N. Shell,* Topological Fields and Near Valuations (1990)
136. *B. F. Doolin and C. F. Martin,* Introduction to Differential Geometry for Engineers (1990)
137. *S. S. Holland, Jr.,* Applied Analysis by the Hilbert Space Method (1990)
138. *J. Oknínski,* Semigroup Algebras (1990)
139. *K. Zhu,* Operator Theory in Function Spaces (1990)
140. *G. B. Price,* An Introduction to Multicomplex Spaces and Functions (1991)
141. *R. B. Darst,* Introduction to Linear Programming (1991)
142. *P. L. Sachdev,* Nonlinear Ordinary Differential Equations and Their Applications (1991)
143. *T. Husain,* Orthogonal Schauder Bases (1991)
144. *J. Foran,* Fundamentals of Real Analysis (1991)
145. *W. C. Brown,* Matrices and Vector Spaces (1991)
146. *M. M. Rao and Z. D. Ren,* Theory of Orlicz Spaces (1991)
147. *J. S. Golan and T. Head,* Modules and the Structures of Rings (1991)
148. *C. Small,* Arithmetic of Finite Fields (1991)
149. *K. Yang,* Complex Algebraic Geometry (1991)
150. *D. G. Hoffman et al.,* Coding Theory (1991)
151. *M. O. González,* Classical Complex Analysis (1992)
152. *M. O. González,* Complex Analysis (1992)
153. *L. W. Baggett,* Functional Analysis (1992)
154. *M. Sniedovich*, Dynamic Programming (1992)
155. *R. P. Agarwal*, Difference Equations and Inequalities (1992)
156. *C. Brezinski*, Biorthogonality and Its Applications to Numerical Analysis (1992)
157. *C. Swartz*, An Introduction to Functional Analysis (1992)
158. *S. B. Nadler, Jr.*, Continuum Theory (1992)
159. *M. A. Al-Gwaiz*, Theory of Distributions (1992)
160. *E. Perry*, Geometry: Axiomatic Developments with Problem Solving (1992)
161. *E. Castillo and M. R. Ruiz-Cobo*, Functional Equations and Modelling in Science and Engineering (1992)
162. *A. J. Jerri*, Integral and Discrete Transforms with Applications and Error Analysis (1992)
163. *A. Charlier et al.*, Tensors and the Clifford Algebra (1992)
164. *P. Biler and T. Nadzieja*, Problems and Examples in Differential Equations (1992)
165. *E. Hansen*, Global Optimization Using Interval Analysis (1992)
166. *S. Guerre-Delabrière*, Classical Sequences in Banach Spaces (1992)
167. *Y. C. Wong*, Introductory Theory of Topological Vector Spaces (1992)
168. *S. H. Kulkami and B. V. Limaye*, Real Function Algebras (1992)
169. *W. C. Brown*, Matrices Over Commutative Rings (1993)
170. *J. Loustau and M. Dillon*, Linear Geometry with Computer Graphics (1993)
171. *W. V. Petryshyn*, Approximation-Solvability of Nonlinear Functional and Differential Equations (1993)

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

172. *E. C. Young*, Vector and Tensor Analysis: Second Edition (1993)
173. *T. A. Bick*, Elementary Boundary Value Problems (1993)
174. *M. Pavel*, Fundamentals of Pattern Recognition: Second Edition (1993)
175. *S. A. Albeverio et al.*, Noncommutative Distributions (1993)
176. *W. Fulks*, Complex Variables (1993)
177. *M. M. Rao*, Conditional Measures and Applications (1993)
178. *A. Janicki and A. Weron*, Simulation and Chaotic Behavior of $\alpha$-Stable Stochastic Processes (1994)
179. *P. Neittaanmäki and D. Tiba*, Optimal Control of Nonlinear Parabolic Systems (1994)
180. *J. Cronin*, Differential Equations: Introduction and Qualitative Theory, Second Edition (1994)
181. *S. Heikkilä and V. Lakshmikantham*, Monotone Iterative Techniques for Discontinuous Nonlinear Differential Equations (1994)
182. *X. Mao*, Exponential Stability of Stochastic Differential Equations (1994)
183. *B. S. Thomson*, Symmetric Properties of Real Functions (1994)
184. *J. E. Rubio*, Optimization and Nonstandard Analysis (1994)
185. *J. L. Bueso et al.*, Compatibility, Stability, and Sheaves (1995)
186. *A. N. Michel and K. Wang*, Qualitative Theory of Dynamical Systems (1995)
187. *M. R. Darnel*, Theory of Lattice-Ordered Groups (1995)
188. *Z. Naniewicz and P. D. Panagiotopoulos*, Mathematical Theory of Hemivariational Inequalities and Applications (1995)
189. *L. J. Corwin and R. H. Szczarba*, Calculus in Vector Spaces: Second Edition (1995)
190. *L. H. Erbe et al.*, Oscillation Theory for Functional Differential Equations (1995)
191. *S. Agaian et al.*, Binary Polynomial Transforms and Nonlinear Digital Filters (1995)
192. *M. I. Gil'*, Norm Estimations for Operation-Valued Functions and Applications (1995)
193. *P. A. Grillet*, Semigroups: An Introduction to the Structure Theory (1995)
194. *S. Kichenassamy*, Nonlinear Wave Equations (1996)
195. *V. F. Krotov*, Global Methods in Optimal Control Theory (1996)
196. *K. I. Beidar et al.*, Rings with Generalized Identities (1996)
197. *V. I. Arnautov et al.*, Introduction to the Theory of Topological Rings and Modules (1996)
198. *G. Sierksma*, Linear and Integer Programming (1996)
199. *R. Lasser*, Introduction to Fourier Series (1996)
200. *V. Sima*, Algorithms for Linear-Quadratic Optimization (1996)
201. *D. Redmond*, Number Theory (1996)
202. *J. K. Beem et al.*, Global Lorentzian Geometry: Second Edition (1996)
203. *M. Fontana et al.*, Prüfer Domains (1997)
204. *H. Tanabe*, Functional Analytic Methods for Partial Differential Equations (1997)
205. *C. Q. Zhang*, Integer Flows and Cycle Covers of Graphs (1997)
206. *E. Spiegel and C. J. O'Donnell*, Incidence Algebras (1997)
207. *B. Jakubczyk and W. Respondek*, Geometry of Feedback and Optimal Control (1998)
208. *T. W. Haynes et al.*, Fundamentals of Domination in Graphs (1998)
209. *T. W. Haynes et al.*, Domination in Graphs: Advanced Topics (1998)
210. *L. A. D'Alotto et al.*, A Unified Signal Algebra Approach to Two-Dimensional Parallel Digital Signal Processing (1998)
211. *F. Halter-Koch*, Ideal Systems (1998)
212. *N. K. Govil et al.*, Approximation Theory (1998)
213. *R. Cross*, Multivalued Linear Operators (1998)
214. *A. A. Martynyuk*, Stability by Liapunov's Matrix Function Method with Applications (1998)
215. *A. Favini and A. Yagi*, Degenerate Differential Equations in Banach Spaces (1999)
216. *A. Illanes and S. Nadler, Jr.*, Hyperspaces: Fundamentals and Recent Advances (1999)
217. *G. Kato and D. Struppa*, Fundamentals of Algebraic Microlocal Analysis (1999)
218. *G. X.-Z. Yuan*, KKM Theory and Applications in Nonlinear Analysis (1999)
219. *D. Motreanu and N. H. Pavel*, Tangency, Flow Invariance for Differential Equations, and Optimization Problems (1999)
220. *K. Hrbacek and T. Jech*, Introduction to Set Theory, Third Edition (1999)
221. *G. E. Kolosov*, Optimal Design of Control Systems (1999)
222. *N. L. Johnson*, Subplane Covered Nets (2000)
223. *B. Fine and G. Rosenberger*, Algebraic Generalizations of Discrete Groups (1999)
224. *M. Väth*, Volterra and Integral Equations of Vector Functions (2000)
225. *S. S. Miller and P. T. Mocanu*, Differential Subordinations (2000)

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

226. *R. Li et al.*, Generalized Difference Methods for Differential Equations: Numerical Analysis of Finite Volume Methods (2000)
227. *H. Li and F. Van Oystaeyen*, A Primer of Algebraic Geometry (2000)
228. *R. P. Agarwal*, Difference Equations and Inequalities: Theory, Methods, and Applications, Second Edition (2000)
229. *A. B. Kharazishvili*, Strange Functions in Real Analysis (2000)
230. *J. M. Appell et al.*, Partial Integral Operators and Integro-Differential Equations (2000)
231. *A. I. Prilepko et al.*, Methods for Solving Inverse Problems in Mathematical Physics (2000)
232. *F. Van Oystaeyen,* Algebraic Geometry for Associative Algebras (2000)
233. *D. L. Jagerman*, Difference Equations with Applications to Queues (2000)
234. *D. R. Hankerson et al.,* Coding Theory and Cryptography: The Essentials, Second Edition, Revised and Expanded (2000)
235. *S. Dăscălescu et al.*, Hopf Algebras: An Introduction (2001)
236. *R. Hagen et al.*, C*-Algebras and Numerical Analysis (2001)
237. *Y. Talpaert*, Differential Geometry: With Applications to Mechanics and Physics (2001)
238. *R. H. Villarreal*, Monomial Algebras (2001)
239. *A. N. Michel et al.,* Qualitative Theory of Dynamical Systems, Second Edition (2001)
240. *A. A. Samarskii*, The Theory of Difference Schemes (2001)
241. *J. Knopfmacher and W.-B. Zhang,* Number Theory Arising from Finite Fields (2001)

Additional Volumes in Preparation

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

# PREFACE

Since the first author's monograph *Analytic Arithmetic of Algebraic Function Fields* was published twenty years ago, some remarkable advances have been made in many directions in this area, particularly regarding abstract prime number theorems, the theory of additive formations, mean–value theorems for multiplicative functions, the probabilistic theory of distribution of values of additive functions, as well as the theory of factorization of polynomials over finite fields, Ramanujan expansions etc. We now have a rather mature and rich theory which is well developed, and it is therefore time to give a readable account of the theory in a new book.

This new book aims to give a comprehensive treatment of the subject, starting with the now classical results of the first author and moving all the way to the latest contributions to research in the area, many of which are due to the second author.

The book focuses strongly on abstract prime number theorems, mean-value theorems of multiplicative functions, and the normal distribution of values of additive functions. These topics are covered in Chapters 3, 5, 6, and 7, which include many new results obtained only in the past twenty years. The material in the older monograph is reviewed, updated and treated in detail in Chapters 1, 2, and 4, mainly. In mathematics, the theory which is exposed here diverges strongly from classical analytic number theory in its *alternative* abstract prime number theorems. The whole of Chapter 5 is devoted to *this* important aspect of the subject.

The style of the last chapter, Chapter 8, is quite different from that of previous chapters in the sense that it is a survey of significant results in some topics not covered in previous chapters. This survey may compensate for the incompleteness of the main discussion regarding those aspects of the theory which are not fully treated.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Last we observe that this book is not only a collection of distinct theorems, proven separately. The authors have tried to organize theorems relevant to each other in appropriate groups, through discussions of relationships amongst the results. Readers may find many new facts in this aspect of the treatment, which are not exposed in the original papers.

As the interest in number theory arising from finite fields has steadily increased in recent years, readers in different areas of pure and applied mathematics, in computer science, and in other sciences and technologies may also find this book quite useful. It could also be used as a graduate textbook and has the advantage of bringing the reader right to the present cutting edge of research in this area.

The first author thanks Richard Warlimont and the author's son, Arnold Knopfmacher, for much fruitful research collaboration. Also, he expresses his appreciation of and admiration for Richard Warlimont, for generously providing advance copies of his many major contributions to this area and for his kind interest in and helpful comments on this project.

The authors also wish to thank Marcel Dekker, Inc., for its interest in publishing this book and Ingrid Eitzen for her careful typing of the manuscript.

John Knopfmacher

Wen-Bin Zhang

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

# CONTENTS

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

# INTRODUCTION

This book may be regarded as essentially a revised and much enlarged new edition of the first author's monograph *Analytic Arithmetic of Algebraic Function Fields*[1]. It is intended as an introduction to one branch of the wider topic of *Abstract Analytic Number Theory* treated in the first author's earlier book, with the latter title[2]. Although this aspect of the subject was not discussed in [AB], it appears to be a fundamental one for the type of theory concerned. It provides in many ways a parallel, in the context of polynomial rings and algebraic function fields over finite fields, as well as certain related systems, to the kind of analytic number theory appropriate to ordinary integers, algebraic number fields, and corresponding further mathematical systems. At the same time, the present results are frequently of a *more precise* nature than their more classical counterparts relating to integers, number fields, and so on.

The possibility of developing an arithmetical theory based mainly on the foundation of the axiom referred to here as *Axiom* $\mathcal{A}^{\#}$ seems to have first been pointed out in papers by Fogels [1]. However, in these papers, Fogels dealt only with some very special (though non–trivial) consequences of Axiom $\mathcal{A}^{\#}$, and referred only to polynomial rings and algebraic function fields over finite fields in order to motivate the axiom. The approach of the present monograph is somewhat different in that:

(i) it investigates a variety of more basic number–theoretical consequences of Axiom $\mathcal{A}^{\#}$ (in some cases together with an additional assumption),

[1] See the bibliography – for simplicity, this book shall be referred to throughout as [ANAL]. However, although for completeness a few academic comparisons with [ANAL] are sometimes included below, a knowledge of or access to [ANAL] is **not required** for a reading of the new book below.

[2] See bibliography – this book will be denoted by [AB].

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

(ii) it shows how further concrete motivation for introducing the axiom is provided by various *asymptotic enumeration theorems* regarding finite modules and certain kinds of finite algebras over principal orders in algebraic function fields, and

(iii) it attempts to lay stress on the fact that the application of arithmetical consequences of Axiom $\mathcal{A}^{\#}$ to objects such as modules or algebras then gives rise to a variety of further enumeration theorems concerning such entities, which were not known previously.

Put in a different way, the main objective in introducing and developing the axiomatic discussion below is (as in [AB]) in order to unify (and simplify) the treatment of certain "arithmetical" phenomena which occur naturally in a multiplicity of contexts, some of which are not usually viewed in a number–theoretical way. The main axiomatics are *not* introduced for the sake of generalization alone, although sometimes weaker hypotheses are introduced simply in order to explore the theoretical ramifications of certain types of conclusions.

The derivation of further concrete enumeration theorems emphasized in point (iii) above amounts in each case to applying some abstract arithmetical proposition based on Axiom $\mathcal{A}^{\#}$ to a specific mathematical system which has been shown to fall under the scope of Axiom $\mathcal{A}^{\#}$ as the consequence of some (non–trivial) asymptotic enumeration theorem. Given the detailed description of natural examples of such systems appearing in Section 1.1 below, such a deduction becomes straight–forward. For this reason, even though (as in similar cases in [AB]) such deductions constitute a major aim of this monograph, they will normally *not be spelled out explicitly.* Similarly, special instances of apparently new abstract theorems will not usually be pointed out individually. As far as the authors are aware, many of the results below had not previously been published in books or journals (neither in abstract nor in "applied" form) before the appearance of [ANAL], and several others appear for the first time in this book or have not appeared previously in book form.

Regarding *prerequisites for reading* the later text, despite the above remarks about new results, it has been designed to be as easily accessible as possible to readers at the beginning graduate level in mathematics. No initial knowledge of the area is assumed, apart from that arising from an elementary reading of ordinary number theory. However a brief perusal of the Introduction to and Chapter 1 of [AB] might be helpful. Although periodic references are made to [AB], most of these are for purposes of technical comparison only, or else quote results which could at least be accepted without proof on a first reading. Thus a full preliminary knowledge of [AB] is definitely *not* required, if occasional quotations from [AB] are accepted without proof initially. Further, so as to keep the development as self-contained as possible, the essential initial concepts will be recalled in detail as they become required below, and the subject will to a large extent be developed *ab initio*, subject to the preceding comments. Two further sets of comments relating to prerequisites seem desirable:

Firstly, in keeping with the aims outlined above, we have attempted to keep the discussion as elementary as possible in the early and some later sections, from the point of view of *real* and *complex analysis*. Thus complex analysis is often either avoided, or kept to a moderate level when its introduction really seems desirable.

Secondly, there is an important point connected with prerequisites concerns algebraic function fields, and topics in algebra. The present monograph covers some aspects of the analytic "arithmetic" of algebraic function fields, polynomials, and certain related systems of modules and algebras over finite fields, but it does *not* attempt to provide a detailed and comprehensive introduction to either function fields and their "zeta" functions, or to the theory of finite modules and algebras connected with function fields. Since much of our basic concrete motivation for introducing and in-

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

vestigating consequences of Axiom $\mathcal{A}^{\#}$ below stems from information about the preceding entities, it has been necessary (in order not to contradict the earlier remarks about minimal prerequisites) to include an *outline* of a few relevant known facts about such matters. (References to fuller treatments of these preliminary facts are provided at the appropriate stages, but particular mention may be made for example to the books by Deuring [1], Eichler [1], Jacobson [1] and Thomas [1].) Although the outline of initial facts just referred to covers some quite advanced topics, a detailed understanding of the background to these matters is *not* required in order to appreciate the motivation for Axiom $\mathcal{A}^{\#}$, or in order to follow the axiomatic development thereafter. In addition, some preliminary remarks in Section 1.1 about polynomial rings over finite fields, and modules over such rings, require *no* advanced knowledge and should in themselves provide reasonable partial motivation for the abstract discussion.

In connection with the further development of this subject, it may be remarked that, in addition to the actual topics treated below, many other aspects of classical–type analytic number theory (relating to the Axiom $\mathcal{A}$ in [AB]) may be expected to have (sometimes sharper) counterparts in the present setting. A few further developments and some open questions or research projects in this direction are surveyed in the final Chapter 8 below.

# CHAPTER 1

# ADDITIVE ARITHMETICAL SEMIGROUPS AND AXIOM $\mathcal{A}^{\#}$

## 1.1 Basic Concepts and Examples

Polynomial rings and algebraic function fields in one variable over a finite field $\mathbb{F}_q$, as well as certain classes of finite modules and algebras connected with these, provide reasonable motivation for studying consequences of a particular *Axiom* $\mathcal{A}^{\#}$ concerning the asymptotic behaviour of certain kinds of arithmetical semigroups discussed below. This monograph deals particularly with consequences of Axiom $\mathcal{A}^{\#}$ with respect to asymptotic average values of arithmetical functions, and regarding asymptotic densities of sets of special "arithmetical" or number–theoretical interest. In addition, in the process of establishing the validity of Axiom $\mathcal{A}^{\#}$ for suitable semigroups relating to special types of modules and algebras, it includes various asymptotic enumeration theorems regarding isomorphism classes, which have some *intrinsic* interest independent of the present abstract arithmetical context. (As emphasized implicitly in the Introduction, the application of consequences of Axiom $\mathcal{A}^{\#}$ to semigroups connected with modules and algebras often provides *further* non–obvious enumeration theorems for such objects.)

In order to formulate the basic axiom in question, first recall (cf. [AB], page 11) that an **arithmetical semigroup** is by definition a commutative semigroup $\mathcal{G}$ with identity element 1, which contains a countable subset $\mathcal{P}$ such that every element $a \neq 1$ in $G$ admits unique factorization into a finite

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

product of powers of elements of $\mathcal{P}$, together with a real-valued mapping $|\ |$ on $\mathcal{G}$ such that:

(i) $|1| = 1,\ |p| > 1$ for $p \in \mathcal{P}$,

(ii) $|ab| = |a|\,|b|$ for all $a,\ b \in \mathcal{G}$,

(iii) the total number $N(x)$ of elements $a$ with $|a| \leq x$ is finite, for each $x > 0$.

The elements of $\mathcal{P}$ are called the *primes* of $\mathcal{G}$, and $|\ |$ is called the *norm* mapping on $\mathcal{G}$. It is obvious that, corresponding to any fixed constant $c > 1$, the definition $\partial(a) = \log_c |a|$ yields a mapping $\partial$ on $\mathcal{G}$ such that:

(i) $\partial(1) = 0,\ \partial(p) > 0$ for $p \in \mathcal{P}$,

(ii) $\partial(ab) = \partial(a) + \partial(b)$ for all $a,\ b \in \mathcal{G}$,

(iii) the total number $N^{\#}(x)$ of elements $a$ with $\partial(a) \leq x$ is finite, for each $x > 0$.

Conversely, any real-valued mapping $\partial$ with the last three properties yields a norm on $\mathcal{G}$, if one defines $|a| = c^{\partial(a)}$. In cases where such a mapping $\partial$ is of primary interest, we call $\mathcal{G}$ together with $\partial$ an **additive** arithmetical semigroup, and refer to $\partial$ as the *degree* mapping on $\mathcal{G}$; compare [AB] page 56. In particular, because it suffices for all the natural examples cited below, *throughout this monograph* (unless otherwise stated) *it shall be assumed* that the symbol $\mathcal{G}$ denotes an *additive* arithmetical semigroup relative to an *integer-valued* degree mapping $\partial$.

In these circumstances, we shall be particularly concerned with arithmetical consequences of assumptions about the total number $G^{\#}(n)$ or $G(n)$ of elements of degree $n$ in $\mathcal{G}$, or about the total number $P^{\#}(n)$ or $P(n)$ of

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

primes of degree $n$ in $\mathcal{G}$. For convenience below, *unlike* the usage in [AB] and [ANAL], the simplified notations $G(n)$ and $P(n)$ will *usually replace* $G^{\#}(n)$ and $P^{\#}(n)$, respectively, *in this book.* On the basis of the motivation supplied by numerous natural examples to be listed below, the main emphasis in this book will be on semigroups satisfying

**Axiom $\mathcal{A}^{\#}$:** *There exist constants $A > 0$, $q > 1$, and $\nu$ with $0 \leq \nu < 1$ (all depending on $\mathcal{G}$, such that*

$$G(n)( = G^{\#}(n)) = Aq^n + 0(q^{\nu n}) \textit{ as } n \to \infty.$$

As in [AB], our main purpose in investigating arithmetical consequences of axioms on the asymptotic behaviour of arithmetical semigroups is to obtain conveniently unified derivations of results that are valid for reasonably large classes of concrete semigroups that occur naturally in various contexts. The following are examples of semigroups satisfying Axiom $\mathcal{A}^{\#}$.

(1.1.1) EXAMPLE: **Galois polynomial rings.** Let $\mathbb{F}_q[X]$ denote a polynomial ring in an indeterminate $X$ over the finite Galois field $\mathbb{F}_q$ with $q$ elements ($q$ a prime–power)[3]. The subset $\mathcal{G}_q = \mathcal{G}(q, X)$ consisting of all *monic* polynomials in $\mathbb{F}_q[X]$ forms a semigroup under multiplication, which may be identified essentially with the semigroup of all associate classes of non–zero elements in $\mathbb{F}_q[X]$ discussed briefly in [AB], Chapter 3. In particular, $\mathcal{G}_q$ together with the usual degree mapping on polynomials forms an additive arithmetical semigroup such that

$$G_q^{\#}(n) = q^n \quad (n = 0, 1, 2, \ldots).$$

[3] Note that, in Axiom $\mathcal{A}^{\#}$, the constant $q$ need *not* necessarily be a prime–power or an integer. However, little would be lost in assuming $q$ to be a prime–power, since this is the case in all the cited examples.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

(1.1.2) EXAMPLE: **Finite modules over $\mathbb{F}_q[X]$.** Let $\mathcal{F}_q$ denote the category of all *finitely-generated torsion modules* over the above ring $\mathbb{F}_q[X]$. The ring $\mathbb{F}_q[X]$ is a principal ideal domain, and thus a quite explicit description of the modules in $\mathcal{F}_q$ may be deduced from the well known theory of finitely-generated modules over principal ideal domains. In particular, $\mathcal{F}_q$ satisfies the Krull–Schmidt theorem, and the *indecomposable* modules in $\mathcal{F}_q$ are essentially the various cyclic modules of type $\mathbb{F}_q[X]/(p^r)$, where $p$ denotes a prime (irreducible) polynomial in $\mathbb{F}_q[X]$, and $r$ is a positive integer. Further, if $f$ denotes an arbitrary polynomial of degree $n > 0$ in $\mathbb{F}_q[X]$, it follows easily from the division algorithm in $\mathbb{F}_q[X]$ that the quotient ring (or module) $\mathbb{F}_q[X]/(f)$ contains exactly $q^n$ elements. Thus the preceding remark about the structure of modules in $\mathcal{F}_q$ implies that every module in $\mathcal{F}_q$ is finite of cardinal some power of $q$, that $\mathcal{F}_q$ coincides with the category of *all* (unital) *modules of finite cardinal* over $\mathbb{F}_q[X]$, and that the total number $\mathcal{F}_q(n)$ of non-isomorphic modules of cardinal $q^n$ in $\mathcal{F}_q$ is finite for each $n = 0, 1, 2, \ldots$.

Thus, relative to the degree function $\partial(M) = \log_q \operatorname{card}(M)$ $\{M \text{ in } \mathcal{F}_q\}$, $\mathcal{F}_q$ forms an *additive arithmetical category* as defined in [AB], page 56. In Section 2.1 below, we shall prove that the associated additive arithmetical semigroup consisting of the set of all isomorphism classes of modules in $\mathcal{F}_q$ satisfies Axiom $\mathcal{A}^{\#}$, and in fact

$$\mathcal{F}_q(n) = P_0(q^{-1})q^n + 0\left(q^{\frac{1}{2}n}\right) \text{ as } n \to \infty,$$

where $P_0(y) = \prod_{r=1}^{\infty}(1 - y^r)^{-1}$ is the classical generating function for *arithmetical partitions* (cf. [AB], page 63, say). Thus here, as indicated earlier, verification of the relevant asymptotic axiom amounts to establishing an *asymptotic enumeration theorem* which has some interest independent of any abstract number-theoretical considerations. Similar remarks apply to many of the other natural examples to be considered later, and in fact most

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

of the general comments on motivation for the relevant abstract theories, that were made in [AB] (for example, in its Introduction), may be applied without essential change to the abstract discussion below. (At the same time, as with [AB], a reader *need not be deterred* from proceeding with the general treatment because of a lack of familiarity with all aspects of the individual concrete examples listed – although there has been no attempt here at indicating more than an *outline* of the detailed mathematical foundations underlying our motivating examples, only a cursory awareness of their nature is required for a first reading.)

(1.1.3) EXAMPLE: **Semisimple finite algebras over $\mathbb{F}_q[X]$.** Let $D$ denote an integral domain. By a *$D$-algebra*, we understand a (unital) $D$-module $A$ which is simultaneously an associative ring, and satisfies: $\lambda(xy) = (\lambda x)y = x(\lambda y)$ for all $\lambda \in D$, and $x$, $y \in A$. In the theory of such algebras, a particularly well understood class is that of the *semi-simple* algebras subject to a descending chain condition; see Jacobson [1], Chapter 4. In particular, letting $\mathcal{S} = \mathcal{S}_D$ denote the class of all *semi-simple $D$-algebras of finite cardinal*, the standard structure theory implies that every algebra in $\mathcal{S}$ has a unique expression (up to isomorphism and rearrangement) as a direct sum of simple finite $D$-algebras. Here a *simple* $D$-algebra is an algebra in which not all products are zero, which contains no proper ideals that are simultaneously submodules, and it is a consequence of standard theory that every simple $D$-algebra of finite cardinal reduces to a total matrix algebra $M_n(F)$ over a finite $D$-algebra $F$ which is a field. In the case when $D$ is the polynomial ring $\mathbb{F}_q[X]$, it can be deduced further (cf. say J. Knopfmacher [1,2]) that the simple finite $D$-algebras are isomorphic to the various total matrix algebras $M_n(F_r)$ $[n,\, r = 1, 2, \ldots]$, where $F_r$ denotes a field extension of degree $r$ of the field $F_1 = \mathbb{F}_q[X]/(p)$, for some prime polynomial $p$. Further, if $p$ has degree $m$, it is easy to see that such an algebra $M_n(F_r)$ contains exactly $q^{mrn^2}$ elements.

The above remarks imply that $\mathcal{S}_D$ forms an additive arithmetical category relative to the degree function $\partial(A) = \log_q \operatorname{card}(A)$ $\{A \text{ in } \mathcal{S}_D\}$, when $D = \mathbb{F}_q[X]$. Letting $\mathcal{S}_q$ denote the category $\mathcal{S}_D$ in this case, it will be proved in Section 2.1 below that the associated additive arithmetical semigroup of all isomorphism classes of algebras in $\mathcal{S}_q$ satisfies Axiom $\mathcal{A}^{\#}$, with

$$\mathcal{S}_q(n) = A_q q^n + 0\left(q^{\frac{1}{2}n}\right) \quad \text{as } n \to \infty,$$

where $A_q = \prod_{rm^2>1}(1 - q^{1-rm^2})^{-1}$, and $\mathcal{S}_q(n)$ denotes the total number of non–isomorphic algebras of cardinal $q^n$ in $\mathcal{S}_q$.

(1.1.4) EXAMPLE: **Integral divisors in algebraic function fields.** Let $K$ denote a field of *algebraic functions in one variable* over a finite constant field $\mathbb{F}_q$ with $q$ elements, i.e., let $K$ be an extension field of finite degree over the field of fractions $\mathbb{F}_q(X)$ of the polynomial ring $\mathbb{F}_q[X]$. A fairly extensive class of natural examples of semigroups satisfying Axiom $\mathcal{A}^{\#}$ stems from the theory of such algebraic function fields, and in order to describe such examples we shall need to recall some well known properties of these fields (treated at length in the books of Deuring [1] and Eichler [1], for example).

The polynomial ring $\mathbb{F}_q[X]$ and its field of fractions $\mathbb{F}_q(X)$ are in many ways "arithmetical cousins" of the ring $\mathbb{Z}$ of all rational integers and the field $\mathbb{Q}$ of all rational numbers. In a similar way, it has long been recognized that algebraic function fields like $K$ above are in many ways natural analogues of ordinary *algebraic number* fields (i.e., extension fields of finite degree over $\mathbb{Q}$. With the exception of special studies relating to the polynomial ring $\mathbb{F}_q[X]$, the derivation of an analogue of Landau's Prime Ideal Theorem, and investigations of a parallel to the Dedekind zeta function of a number field, this "arithmetical" parallel between the two classes of fields has not been pursued very extensively in relation to many questions of analytic number theory. Consequently, a large proportion of the results to be derived later subject to Axiom $\mathcal{A}^{\#}$ appear to be relatively new when applied to algebraic function fields, as well as for the other examples listed above. (However, this comment is partly but less widely applicable to the specializations valid for $\mathbb{F}_q[X]$ also, since here one may also refer to various research papers, such as those of Carlitz [1–3], Carlitz and Cohen [1–2], E. Cohen [1], S.D. Cohen [1–2] and Shader [1], for example; cf. also [AB], Chapter 3.)

The analogue of the Dedekind zeta function of an algebraic number field for a function field $K$ as above is

$$\zeta_K(z) = \sum_{\alpha} N(\alpha)^{-z} = \prod_{\rho} (1 - N(\rho)^{-z})^{-1},$$

where the sum is over all integral divisors $\alpha$ of $K$, $N(\alpha)$ denotes the "absolute norm" of $\alpha$, and the product is over all prime divisors $\rho$; see for example Eichler [1], page 300. It is known (cf. Eichler [1], say) that

$$\zeta_K(z) = -\frac{L(q^{-z})}{(1-q^{-z})(1-q^{1-z})},$$

where $L(q^{-z})$ is a polynomial with rational integer coefficients in $q^{-z}$, whose degree is twice the "genus" of $K$. Further, by a theorem of A. Weil, every zero $z$ of $L(q^{-z})$ has real part $\frac{1}{2}$, i.e., the "Riemann hypothesis" is valid for $\zeta_K(z)$.

By way of illustration it may be noted that the field $K_0 = \mathbb{F}_q(X)$ has the zeta function $\zeta_0(z) = (1 - q^{-z})^{-1}\,(1 - q^{1-z})^{-1}$.

Now let $\mathcal{G}_K$ denote the multiplicative semigroup of all integral divisors of $K$. Then $\mathcal{G}_K$ forms an additive arithmetical semigroup relative to the degree function $\partial(\alpha) = \log_q N(\alpha)$, and (if $K(n)$ denotes the total number of divisors of degree $n$ in $\mathcal{G}_K$) one has

$$\zeta_K(z) = \sum_{n=0}^{\infty} K(n) q^{-nz}.$$

By comparing this with the equation for $\zeta_K(z)$ quoted above, and comparing coefficients, it follows that

$$K(n) = A_K q^n + B \text{ for } n \geq 2g,$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

where $A_K = \frac{q}{q-1}L(q^{-1})$, $2g = \deg L(q^{-z})$, and $B$ is a constant. Thus

$$K(n) = A_K q^n + O(1) \text{ as } n \to \infty,$$

and hence $\mathcal{G}_K$ satisfies Axiom $\mathcal{A}^{\#}$. (Although the fact will not be used here, it may be interesting to remark that the polynomial $L(q^{-z})$ is known to satisfy a certain functional equation relative to the substitution $z \to 1 - z$ which implies that $L(q^{-1}) = q^{-g}h$, where $h$ is the "class number" of $K$.)

(1.1.5) EXAMPLE: **Ideals in the principal order of an algebraic function field.** Let $D$ denote the *ring of integral functions* in the algebraic function field $K$ discussed above, i.e., the principal order in $K$ with respect to $\mathbb{F}_q[X]$; for later purposes, it will be convenient to refer to $D$ simply as *the* principal order in $K$. Unlike the situation in algebraic number theory, the theory of the non-zero ideals within $D$ does not quite coincide with that of the integral divisors in $K$. The distinction arises from the (finite) set of prime divisors of $K$ induced by the denominator divisor of $X$ in $\mathbb{F}_q(X)$; the set $\mathcal{G}_D$ of all non-zero ideals of the ring $D$ may be identified essentially with all those integral divisors of $K$ that are not divisible by any of these particular prime divisors. Thus $\mathcal{G}_D$ forms a sub-semigroup of $\mathcal{G}_K$, and it turns out that the absolute norm $N(\alpha)$ of an ideal $\alpha$ in $\mathcal{G}_D$ is equal to the *total number of elements of the quotient ring* $D/\alpha$; cf. Eichler [1], page 300.

Now let $D(n)$ denote the total number of ideals of *degree* $n$ in $D$, i.e., ideals of absolute norm $q^n$. Then, as in [AB], Chapter 3, it may be deduced that (relative to the absolute norm) the arithmetical semigroup $G_D$ has the zeta function

$$\zeta_D(z) = \sum_{n=0}^{\infty} D(n)q^{-nz} = \prod_{\rho} \left(1 - N(\rho)^{-z}\right)^{-1},$$

where the product is over all prime ideals $\rho$ in $D$. Thus

$$\zeta_D(z) = \zeta_K(z) \prod_{\rho} \left(1 - N(\rho)^{-z}\right),$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

where the last product is over the finite set of prime divisors of $K$ arising from the "denominator divisor" of $X$ in $\mathbb{F}_q(X)$. By the formulae for $\zeta_K(z)$ quoted earlier, it therefore follows that

$$\zeta_D(z) = \frac{\mathbb{Q}(q^{-z})}{1 - q^{1-z}},$$

where $\mathbb{Q}(q^{-z})$ is also a polynomial with rational integer coefficients in $q^{-z}$. By equating coefficients of the powers of $q^{-z}$, this implies that $D^{\#}(n) = \mathbb{Q}(q^{-1})q^n$ for $n \geq M$, where $M = \deg \mathbb{Q}(q^{-z})$. Thus

$$D(n) = A_D q^n + O(1) \text{ as } n \to \infty,$$

where $A_D = \mathbb{Q}(q^{-1})$; compare Example 1.1.1 above, which is essentially the special case of the present example that occurs when $K = \mathbb{F}_q(X)$.

The fact that the semigroup $\mathcal{G}_D$ satisfies Axiom $\mathcal{A}^{\#}$ will turn out later on to be particularly significant for the purpose of establishing both asymptotic enumeration theorems, and the validity of Axiom $\mathcal{A}^{\#}$, in relation to the following examples:

(1.1.6) EXAMPLE: **Finite modules over a ring of integral functions.** Let $\mathcal{F} = \mathcal{F}_D$ denote the category of all *finitely-generated torsion modules* over the ring $D$ of "integral functions" considered above; when $D = \mathbb{F}_q[X]$, $\mathcal{F}_D$ reduces to the category $\mathcal{F}_q$ of Example 1.1.2. In the general case, $D$ is a domain of the kind treated in the book of Jacobson [1], Chapter 6, and the module theory developed there implies that $\mathcal{F}$ is a category satisfying the Krull–Schmidt theorem, and that the *indecomposable* modules in $\mathcal{F}$ are isomorphic to the various cyclic modules $D/\rho^r$, where $\rho$ is a prime ideal in $D$ and $r$ is a positive integer. By an earlier assertion about the absolute norm of an ideal in $\mathcal{G}_D$, it follows that such a module $D/\rho^r$ contains exactly $N(\rho)^r$ elements.

In view of the above remarks, it is not hard to deduce that $\mathcal{F}$ coincides with the category of all (unital) modules of *finite cardinal* over $D$, and

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

$\mathcal{F}$ forms an additive arithmetical category relative to the degree function $\partial(M) = \log_q \operatorname{card}(M)$ $\{M$ in $\mathcal{F}\}$. It follows from an asymptotic theorem regarding $\mathcal{F}$ to be proved later that the associated additive arithmetical semigroup of all isomorphism classes of modules in $\mathcal{F}$ satisfies Axiom $\mathcal{A}^{\#}$.

(1.1.7) EXAMPLE: **Semisimple finite algebras over a ring of integral functions.** Consider the category $\mathcal{S} = \mathcal{S}_D$ discussed in Example 1.1.3 above, in the case when $D$ is the present ring of integral functions in the field $K$. Then (cf. say J. Knopfmacher [1,2]) the description of the *simple* $D$-algebras given earlier for the case when $D = \mathbb{F}_q[X]$ can be shown to extend to the present more general case in such a way that they may now be listed (up to isomorphism) as the various total matrix algebras $M_n(F_r)[n, r = 1, 2, \ldots]$, where $F_r$ denotes a field extension of degree $r$ of the finite field $F_1 = D/\rho$ $\{\rho$ a prime ideal in $D\}$; here $M_n(F_r)$ has cardinal $N(\rho)^{rn^2}$. Thus, relative to the degree function $\partial(B) = \log_q \operatorname{card}(B)$ $\{B$ in $\mathcal{S}\}$, $\mathcal{S}$ also forms an additive arithmetical category in the present case, and it will be proved later that its associated arithmetical semigroup also satisfies Axiom $\mathcal{A}^{\#}$.

It is interesting to note that the above natural examples appertaining to Axiom $\mathcal{A}^{\#}$ are the direct polynomial and function field analogues of the main concrete examples of arithmetical semigroups satisfying Axiom $\mathcal{A}$ that were discussed in [AB], Part II, the latter examples being grounded on properties of algebraic number fields. Further, one may in a sense view Axiom $\mathcal{A}^{\#}$ as a kind of "discrete" additive analogue of Axiom $\mathcal{A}$: For, it is easy to verify that Axiom $\mathcal{A}^{\#}$ (in the form stated earlier) is equivalent to the assertion that, as $n \to \infty$,

$$N_G(n) = \sum_{r \leq n} G^{\#}(r) = A'q^n + \begin{cases} O(n) & \text{if } \nu = 0, \\ O(q^{\nu n}) & \text{if } \nu > 0, \end{cases}$$

where $A' = \frac{q}{q-1}A$. Thus, if $\mathcal{G}$ is regarded as an arithmetical semigroup relative to the norm $|a| = q^{\partial(a)}$, Axiom $\mathcal{A}^{\#}$ is equivalent to the assertion

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

that, *as $x \to \infty$ via powers of $q$ alone*,

$$N_G(x) = A'x + \begin{cases} O(\log x) & \text{if } \nu = 0, \\ O(x^{\nu}) & \text{if } \nu > 0. \end{cases}$$

In view of these remarks it is not surprising that many conclusions based on Axiom $\mathcal{A}$ are parallel by conclusions subject to Axiom $\mathcal{A}^{\#}$. However, as will be seen shortly, the consequences of Axiom $\mathcal{A}^{\#}$ often tend to give *more precise* information, and have *simpler* proofs.

We conclude this section with another algebraic example, and a simple proposition showing that every arithmetical semigroup satisfying Axiom $\mathcal{A}^{\#}$ has infinitely many sub–semigroups satisfying the same axiom.

(1.1.8) EXAMPLE: **Homogenous polynomials over $\mathbb{F}_q$.** We thank Arnold Knopfmacher for this example: Let $\mathbb{F}_q[X_1, \ldots, X_k]$ denote a polynomial ring in $k$ indeterminates $X_1, \ldots, X_k$ over $\mathbb{F}_q$. Let $\mathcal{H}_{q,k}$ denote the set of all associate–classes of *homogeneous* polynomials in $\mathbb{F}_q[X_1, \ldots, X_k]$, where two polynomials are called associates if and only if they differ at most by a non–zero factor $\lambda \in \mathbb{F}_q$. If $\partial$ now represents *total degree*, then $\mathcal{H}_{q,k}$ forms an additive arithmetical semigroup with exactly

$$H_{q,k}(n) = \frac{1}{q-1}\left\{q^{\binom{n+k-1}{vk-1}} - 1\right\}$$

elements of degree $n$; this equation follows easily with aid of the standard combinatorial proposition that there are $\binom{n+k-1}{k-1}$ different solutions of the equation $r_1 + r_2 + \cdots + r_k = n$ in non–negative integers $r_i$ (cf. say van Lint and Wilson [1], Chap. 13).

In particular, for $k = 2$, the semigroup $\mathcal{H}_{q,2}$ satisfies Axiom $\mathcal{A}^{\#}$.

(1.1.9) PROPOSITION. *Suppose that $\mathcal{G}$ is an additive arithmetical semigroup satisfying Axiom $\mathcal{A}^{\#}$ as stated above, and let $\mathcal{G}\langle k \rangle$ denote the* *set of all elements of $\mathcal{G}$ that are coprime to a given element $k \in \mathcal{G}$. Then $\mathcal{G}\langle k\rangle$ also forms an arithmetical semigroup satisfying Axiom $\mathcal{A}^{\#}$, and (with self-explanatory notation) as $n \to \infty$*

$$G\langle k\rangle(n) = Aq^n \prod_{\textit{prime } p|k} \left(1 - q^{-\partial(p)}\right) + O(q^{\nu n}).$$

PROOF. First note that $\mathcal{G}\langle 1\rangle = \mathcal{G}$, and that in general $\mathcal{G}\langle k\rangle$ is a sub-semigroup of $\mathcal{G}$ depending only the distinct primes $p_1, \ldots, p_m$ dividing $k$. Then observe that, for a prime $p \in \mathcal{P}$,

$$\begin{aligned} G\langle p\rangle(n) &= G(n) - \sum_{\partial(a)=n,\, p|a} 1 = G(n) - \sum_{\partial(pb)=n} 1 \\ &= G(n) - G(n - \partial(p)) = A\left(1 - q^{-\partial(p)}\right) q^n + O(q^{\nu n}). \end{aligned}$$

The stated formula for $G\langle k\rangle(n)$ now follows by induction on the number $m$ primes $p_i|k$. □

## 1.2 The Zeta or Generating Function

For the rest of this chapter, unless the contrary is explicitly indicated, $(\mathcal{G}, \partial)$ *shall denote an arbitrary additive arithmetical semigroup satisfying Axiom* $\mathcal{A}^{\#}$ in the form stated earlier. Here properties relating to the degree function $\partial$ are usually of greatest interest, and so most of the discussion will be expressed accordingly.

Since the degree mapping $\partial$ only is assumed to be *integer–valued*, special interest attaches to the counting function $G^{\#}(n)$ or $G(n)$, and $P^{\#}(n)$ or $P(n)$, defined in the previous section for $n = 0, 1, 2, \ldots$. These numbers are inter–related by means of the useful **Euler product formula** for $\mathcal{G}$ below, so named because of its analogy with similar formulae for ordinary integers and algebraic number fields stemming from Euler and (later) Dedekind. A fuller treatment of such formulae for arithmetical semigroups is given in Chapter 3 of [AB], but a simple alternative starting approach should suffice here:

As a matter of temporary convenience, first suppose that $\mathcal{G}$ is an arbitrary arithmetical semigroup with an *integer–valued* norm mapping $|\ |$. Also as *temporary* notations only, let $G'(n)$ denote the total number of elements of $\mathcal{G}$ with norm $n$, and let $P'(n)$ denote the corresponding number of prime elements of $\mathcal{G}$. Then, ignoring questions of convergence initially, note (along lines stemming from Euler) that unique factorization into prime elements implies that the series

$$\begin{aligned}
\zeta_{\mathcal{G}}(z) &= \sum_{n=1}^{\infty} G'(n) n^{-z} = \sum_{a \in \mathcal{G}} |a|^{-z} \\
&= 1 + \sum_{\substack{\text{all products} \\ p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m} \text{ with} \\ p_i \in \mathcal{P},\, r_i \in \mathbb{N},\, m \in \mathbb{N}}} |p_1^{r_1} p_2^{r_2} \ldots p_m^{r_m}|^{-z}
\end{aligned}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

$$= 1 + \sum |p_1|^{-r_1 z}|p_2|^{-r_2 z} \dots |p_m|^{-r_m z}$$

$$= \prod_{p\in\mathcal{P}} \left(1 + |p|^{-z} + |p|^{-2z} + \cdots\right) = \prod_{p\in P} (1 - |p|^{-z})^{-1}$$

$$= \prod_{m=2}^{\infty} (1 - m^{-z})^{-P'(m)}.$$

As a function of $z$, $\zeta_{\mathcal{G}}(z)$ is called the **zeta function** of $\mathcal{G}$, and the last product is its "Euler product" formula. In the case when $\mathcal{G}$ is an *additive* arithmetical semigroup with $|a| = c^{\partial(a)}$ for some integer $c > 1$, one may substitute the symbol $y$ for $c^{-z}$ and directly obtain the **modified** Euler product formula:

$$\sum_{n=0}^{\infty} G^{\#}(n) y^n = \prod_{m=1}^{\infty} (1 - y^m)^{-P^{\#}(m)};$$

then $Z_{\mathcal{G}}(y) = \sum_{n=0}^{\infty} G^{\#}(n) y^n$ is called the **modified zeta**, or **enumerating**, or **generating**, function of $\mathcal{G}$.

Note that when $\mathcal{G}$ satisfies Axiom $\mathcal{A}^{\#}$ and $q$ is also an *integer* then $q$ would be a natural (though not essential) choice for the preceding integer $c > 1$ used in defining the corresponding norm mapping on $\mathcal{G}$. When relevant, such a choice will usually be followed, unless otherwise indicated. (Observe once more that although the constant $q > 1$ of Axiom $\mathcal{A}^{\#}$ is *not* stipulated to be an integer, all the cited natural instances of this axiom involve prime-power values for $q$; hence little would be lost in assuming such an extra condition. Since the abstract development of consequences of Axiom $\mathcal{A}^{\#}$ below centres on properties of an arbitrary but *fixed* additive arithmetical semigroup $\mathcal{G}$ satisfying Axiom $\mathcal{A}^{\#}$, it will be convenient for much of the later discussion in this book to use the *simplified* notations $Z(y)$, $G(n)$ and $P(n)$ for $Z_{\mathcal{G}}(y)$, $G^{\#}(n)$ and $P^{\#}(n)$, respectively. The (modified) *Euler product formula* for $\mathcal{G}$ will then have the appearance

$$Z(y) = \sum_{n=0}^{\infty} G(n) y^n = \prod_{m-1}^{\infty} (1 - y^m)^{-P(m)}.$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

The next proposition deals with the analytical validity of this formula under Axiom $\mathcal{A}^{\#}$, when $y$ takes complex values:

(1.2.1) PROPOSITION. *The radius of convergence of $Z(y)$ is $q^{-1}$, and $Z(y)$ satisfies the above "Euler product" formula analytically and is non–zero when $|y| < q^{-1}$. Further, $Z(y)$ extends to a regular analytic function of $y$ for all complex $y \neq q^{-1}$ in the open disc $|y| < q^{-\nu}$, and has a simple pole with residue $-q^{-1}A$ at $y = q^{-1}$.*

PROOF. Since $G(n) = 0(q^n)$, it is obvious that $Z(y)$ is absolutely convergent for $|qy| < 1$, i.e., $|y| < q^{-1}$. Hence, with any convenient choice of an integer $c > 1$, the corresponding series $\zeta_{\mathcal{G}}(z)$ is absolutely convergent for $Re\, z > 1$. Hence it follows from Corollary 4.2.2 of [AB] that $Z(y)$ satisfies the Euler product formula analytically and is non–zero, when $|y| < q^{-1}$.

Now let $R_n = G(n) - Aq^n$. Then, for $|y| < q^{-1}$,

$$Z(y) = A \sum_{n=0}^{\infty} q^n y^n + \sum_{n=0}^{\infty} R_n y^n = \frac{A}{1 - qy} + \sum_{n=0}^{\infty} R_n y^n.$$

Since $R_n = O(q^{\nu n})$ by Axiom $\mathcal{A}^{\#}$, one sees that the last series represents a regular analytic function of $y$ in the disc $|y| < q^{-\nu}$. Hence the other assertions about $Z(y)$ follows from the preceding formula. □

In parallel with other situations of abstract analytic number theory, it is sometimes useful to have information about the asymptotic behaviour of partial sums of $Z(y)$ for general complex values of $y$:

(1.2.2) PROPOSITION.

*(i) For $|y| < q^{-1}$,*

$$\sum_{n \leq N} G(n) y^n = Z(y) + O(|qy|^N).$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

*(ii)*

$$\sum_{n\leq N} G(n)q^{-n} = AN + \gamma_G + A + O(q^{(\nu-1)N}),$$

*where*

$$\gamma_G = \sum_{n=0}^{\infty} \left\{G(n) - Aq^n\right\} q^{-n} = \lim_{y\to q^{-1}} \left\{Z(y) - \frac{A}{1-qy}\right\}.$$

*(iii)* *For* $|y| \geq q^{-1}$, $y \neq q^{-1}$,

$$\sum_{n\leq N} G(n)y^n = \frac{A(qy)^{N+1}}{qy-1} + \begin{cases} Z(y) + O(|q^\nu y|^N & \textit{if } |y| < q^{-\nu}, \\ O(N) & \textit{if } |y| = q^{-\nu}, \\ O(q^\nu y|^N) & \textit{if } |y| > q^{-\nu}. \end{cases}$$

PROOF.

(i) For $|y| < q^{-1}$,

$$\begin{aligned} \sum_{n\leq N} G(n)y^n &= Z(y) - \sum_{n>N} G(n)y^n = Z(y) + O\left(\sum_{n>N} |qy|^n\right) \\ &= Z(y) + O(|qy|^N), \end{aligned}$$

since $|qy| < 1$.

(ii) Let $R_n = G(n) - Aq^n$. Then, by Axiom $\mathcal{A}^\#$,

$$\begin{aligned} \sum_{n\leq N} G(n)q^{-n} &= \sum_{n\leq N} (Aq^n + R_n)q^{-n} = A(N+1) + \sum_{n\leq N} R_n q^{-n} \\ &= A(N+1) + \sum_{n=0}^{\infty} R_n q^{-n} + O\left(\sum_{n>N} q^{(\nu-1)n}\right) \\ &= AN + \gamma_g + A + O(q^{(\nu-1)N}), \end{aligned}$$

since $\nu < 1$.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

(iii) For $y \neq q^{-1}$,

$$\sum_{n \leq N} G(n) y^n = \frac{A}{qy-1}\left[(qy)^{N+1} - 1\right] + \sum_{n \leq N} R_n y^n.$$

The three cases of assertion (iii) are then easily dealt with, with the aid of elementary properties of geometric progressions. □

It is interesting to note that, relative to the norm on $\mathcal{G}$ defined by some integer $c > 1$, assertion (ii) above implies that the constant $\gamma_G$ satisfies

$$\gamma_G = \lim_{z \to 1}\left\{\zeta_G(z) - \frac{A}{(z-1)\log c}\right\},$$

and

$$\sum_{|a| \leq x} |a|^{-1} = \frac{A}{\log c}\log x + \gamma_G + O(x^{\nu-1})$$

as $x \to \infty$ *via powers of* $c$ *alone.* Therefore the constant $\Gamma_G$ is closely analogous to the *"Euler constant"* of an arithmetical semigroup satisfying Axiom $\mathcal{A}$ (cf. [AB], page 89), and the *same* name may be applied in the present constant. (If convenient, we may also write $\gamma_G = \gamma_{\mathcal{G}}$.)

By way of illustration, consider the Euler constants of the semi-groups $\mathcal{G}_K$ and $\mathcal{G}_D$ discussed in Examples 1.1.4 and 1.1.5 above:

Firstly, by Proposition 1.2.2 (ii),

$$\begin{aligned}\gamma_{\mathcal{G}_K} &= \lim_{y \to q^{-1}}\left\{Z(y) - \frac{A_K}{1-qy}\right\} = \lim_{y \to q^{-1}}\left\{\frac{\frac{L(y)}{1-y} - \frac{qL(q^{-1})}{q-1}}{1-qy}\right\} \\ &= \frac{-q^{-1}}{(1-q^{-1})^2}\left[L(q^{-1}) + (1-q^{-1})L'(q^{-1})\right],\end{aligned}$$

by l'Hôpital's theorem on limits or the definition of a derivative. Similarly,

$$\begin{aligned}\gamma_{\mathcal{G}_D} &= \lim_{y \to q^{-1}}\left\{Z(y) - \frac{A_D}{1-qy}\right\} = \lim_{y \to q^{-1}}\left\{\frac{P(y) - P(q^{-1})}{1-qy}\right\} \\ &= q^{-1}P'(q^{-1}).\end{aligned}$$

In particular, by substitution in the last formula (or by a direct argument) when $D = \mathbb{F}_q[X]$, one finds that the semigroup $\mathcal{G}_q$ of all monic polynomials in $\mathbb{F}_q[X]$ has Euler constant zero. This fact contrasts strongly with the non-triviality of the classical Euler constant $\gamma = 0.57221\ldots$, which arises from the semigroup $\mathbb{N}$ of all positive integers.

The next proposition shows that, for a general semigroup $\mathcal{G}$ as before, *all* the coefficients $\gamma_i = \gamma_i(\mathcal{G})\,(i \geq 0)$ in the Laurent expansion of $Z_G(y)$ about $y = q^{-1}$ satisfy relations of a type analogous to those that occur in Proposition 1.2.2 (ii) for the Euler constant $\gamma_G = \gamma_0$; hence these coefficients may be referred to as the *generalized Euler constants* of $\mathcal{G}$ when $i \geq 1$. (For the analogous theorem subject to Axiom $\mathcal{A}$ of [AB], see J. Knopfmacher [4].)

(1.2.3) PROPOSITION. *Let the Laurent expansion of $Z(y)$ about $y = q^{-1}$ be written in the form*

$$Z(y) = \frac{A}{1-qy} + \sum_{i=0}^{\infty} \gamma_i (y - q^{-1})^i.$$

*Then*

$$\begin{aligned} \gamma_i &= q^i \sum_{n \leq N} \binom{n}{i} \left[G(n)q^{-n} - A\right] + O\left(N^i q^{(\nu-1)N}\right) \\ &= q^i \sum_{n=1}^{\infty} \binom{n}{i} \left[G(n)q^{-n} - A\right]. \end{aligned}$$

PROOF. This proposition is a consequence of Axiom $\mathcal{A}^{\#}$ together with:

(1.2.4) LEMMA. *Let $F(y) = \sum_{n=0}^{\infty} b(n)y^n$ be a power series with coefficients $b(n)$ having the property that there exist constants $B \neq 0$, $x > 1$*

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

*and* $\alpha < 1$, *such that*

$$b(N) = Bx^N + O(x^{\alpha N}) \text{ as } N \to \infty.$$

*Then the radius of convergence of* $F(y)$ *is* $x^{-1}$, *and* $F(y)$ *can be extended to a regular analytic function of* $y$ *for all complex* $y \neq x^{-1}$ *in the open disc* $|y| < x^{-\alpha}$, *in such a way that* $F(y)$ *has a Laurent expansion about* $y = x^{-1}$, *of the form*

$$F(y) = \frac{B}{1-xy} + \sum_{i=0}^{\infty} \beta_i (y - x^{-1})^i,$$

*where*

$$\begin{aligned} \beta_i &= x^i \sum_{n \leq N} \binom{n}{i} \Big[b(n)x^{-n} - B\Big] + O\left(N^i x^{(\alpha-1)N}\right) \\ &= x^i \sum_{n=1}^{\infty} \binom{n}{i} \Big[b(n)x^{-n} - B\Big]. \end{aligned}$$

PROOF. It follows from the asymptotic hypothesis on $b(N)$ that $F(y)$ is absolutely convergent when $|xy| < 1$, i.e., when $|y| < x^{-1}$. Also, similarly to the proof of Proposition 1.2.1, if $r_n = b(n) - Bx^n$ and $|y| < x^{-1}$,

$$F(y) = \frac{B}{1-xy} + \sum_{n=0}^{\infty} r_n y^n,$$

where the last series is absolutely convergent for $|y| < x^{-\alpha}$. Thus $F(y)$ has radius of convergence $x^{-1}$, and about $y = x^{-1}$ the function $g(y) = \sum_{n=0}^{\infty} r_n y^n$ has a Taylor expansion of the form

$$g(y) = \sum_{i=0}^{\infty} \beta_i (y - x^{-1})^i,$$

where

$$\beta_i = g^{(i)}(x^{-1})/i!\,.$$

Now, for $i \geq 0$,

$$\begin{aligned}
\sum_{n \leq N} \binom{n}{i} b(n) x^{i-n} &= Bx^i \sum_{n \leq N} \binom{n}{i} + \sum_{n \leq N} \binom{n}{i} r_n x^{i-n} \\
&= Bx^i \sum_{n \leq N} \binom{n}{i} + \frac{g^{(i)}(x^{-1})}{i!} + O\left( \sum_{n > N} n^i x^{(\alpha-1)n} \right) \\
&= Bx^i \binom{N+1}{i+1} + \beta_i + O\left( N^i x^{(\alpha-1)N} \right),
\end{aligned}$$

with the aid of (Abelian) partial summation, as discussed for example in [AB], Chapter 4, §2. This proves the lemma. □

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

## 1.3 Averages and Densities in Simple Cases

We turn now to initial discussions of the "average values" of arithmetical functions, and of the "densities" of certain subsets of $\mathcal{G}$. Here, any complex-valued function on $\mathcal{G}$ is referred to as an **arithmetical function**, but, as in [AB], our main concern will be with special functions arising from particular number-theoretical considerations.

Given an arithmetical function $f$, the **average-** (or **mean-**) **value** of $f$ for elements of degree $N$ in $\mathcal{G}$ is defined to be $\overline{f}(N)/G(N)$, where $\overline{f}(N) = \sum_{\partial(a)=N} f(a)$. Note that here the bar over $f$ does *not* indicate complex-conjugation; sometimes we may also write $F(n)$ for $\overline{f}(n)$, alternatively, and refer to $F$ or $\overline{f}$ as the **summatory** function associated with $f$. If this average value tends to a finite limit $m = m(f)$ as $N \to \infty$, we shall call $m(f)$ the **asymptotic mean-value** of $f$. If, in addition, $f$ is the characteristic function of some subset $E$ of $\mathcal{G}$, we shall call its asymptotic mean-value $\partial = \partial(E)$ the asymptotic **density** of $E$ in $\mathcal{G}$. (Recall that the *characteristic* function of $E$ is the function that takes value 1 on elements of $E$, and value 0 otherwise.)

Regarding the determination of average values (as in Theorem 3.1 below, for example), attention may and normally will be confined to specifying the asymptotic behaviour of the relevant numbers $\overline{f}(N)$ as $N \to \infty$, since the same denominator $G(N)$ appears throughout and is given asymptotically by Axiom $\mathcal{A}^{\#}$. In this connection, it is also worth noting that the present terminology is consistent with that used in [AB], Chapter 4, in the context of Axiom $\mathcal{A}$:

In order to verify this assertion, note firstly that, if $f$ has a mean-value $m(f)$ in the above sense, then a standard elementary theorem on limits

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

implies that

$$m(f) = \lim_{N\to\infty} \left\{ \sum_{n\le N} \overline{f}(n) \right\} \Big/ \left\{ \sum_{n\le N} G(n) \right\}.$$

Conversely, if the last limit is assumed to exist, the fact that

$$\sum_{n\le N} G(n) \sim \frac{A}{q-1} q^{N+1} \text{ as } N \to \infty$$

implies that

$$\begin{aligned} \overline{f}(N) &= \sum_{n\le N} \overline{f}(n) - \sum_{n\le N-1} \overline{f}(n) \\ &\sim \frac{A}{q-1} m(f) \left[ q^{N+1} - q^N \right] = Am(f)q^N \text{ as } N \to \infty; \end{aligned}$$

thus $m(f)$ is also the asymptotic mean–value of $f$ in the present sense.

(1.3.1) THEOREM. *Let $f$, $g$ be arithmetical functions such that*[4]

$$f^{\#}(y) = [Z(y)]^k g^{\#}(y),$$

*where $k$ is a positive integer, and $g^{\#}(y)$ is absolutely convergent for $|y| < q^{\tau}$, $\tau > -1$. Then as $n \to \infty$,*

$$\overline{f}(N) = \frac{A^k}{(k-1)!} \left[ g^{\#}(q^{-1}) + o(1) \right] N^{k-1} q^N.$$

*In particular, if $k = 1$, $f$ has the mean–value $g^{\#}(q^{-1})$.*

PROOF. First consider the case when $f$ is the *generalized divisor function* $d_k$ such that $d_k(a) = \sum_{b_1 b_2 \ldots b_k = a} 1\{a \in \mathcal{G}\}$:

[4] Here, and later on, repeated use will be made of the **associated power series** or **generating–function** of $f$: $f^{\#}(y) = \sum_{n=0}^{\infty} \overline{f}(n) y^n$ of a given arithmetical function $f$.

(1.3.2) LEMMA. *For $k \geq 2$,*

$$\overline{d_k}(N) = \frac{A^k}{(k-1)!} N^{k-1} q^N + O(N^{k-2} q^N) \text{ as } N \to \infty.$$

PROOF. By Theorem 3.3.1 of [AB], $d_k^{\#}(y) = [Z(y)]^k$. The lemma will be proved by induction, starting with the *divisor* function $d = d_2$. Since $d^{\#}(y) = [Z(y)]^2$,

$$\begin{aligned} \overline{d}(N) &= \sum_{r=0}^{N} G(r) G(N-r) = \sum_{r=0}^{N} [Aq^r + O(q^{\nu r})] \left[Aq^{N-r} + O(q^{\nu(N-r)})\right] \\ &= A^2(N+1)q^N + \sum_{r=0}^{N} \left\{O(q^{N+r(\nu-1)}) + O(q^{\nu N + r(1-\nu)}) + O(q^{\nu N})\right\} \\ &= A^2(N+1)q^N + O(q^N) + O(Nq^{\nu N}), \end{aligned}$$

which proves the lemma for $k = 2$.

Now let $k > 2$, and assume that the lemma has already been proved for $d_{k-1}$. Then the formula $d_k^{\#}(y) = d_{k-1}^{\#}(y) Z(y)$ implies that

$$\overline{d_k}(N) = \sum_{r=0}^{N} \overline{d_{k-1}}(r) G(N-r) = \sum_{r=0}^{N} \left[Br^{k-2} q^r + O(r^{k-3} q^r)\right] \left[Aq^{N-r} + O(q^{\nu(N-r)})\right],$$

where $B = A^{k-1}/(k-2)!$. Therefore

$$\begin{aligned} \overline{d_k}(N) &= \sum_{r=0}^{N} \left\{ABq^N r^{k-2} + O(r^{k-2} q^{\nu N + r(1-\nu)}) + O(r^{k-3} q^N) + O(r^{k-3} q^{\nu N + r(1-\nu)})\right\} \\ &= ABq^N \left\{\frac{N^{k-1}}{k-1} + O(N^{k-2})\right\} + O(N^{k-2} q^N). \end{aligned}$$

by the elementary estimate:

$$\sum_{r \leq N} r^m = \frac{N^{m+1}}{m+1} + O(N^m) \quad [m = 1, 2, \ldots].$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

This proves the lemma. □

(1.3.3) COROLLARY. *The average value of the divisor function $d$ for elements of degree $N$ in $\mathcal{G}$ is equal to*

$$AN + O(1) \text{ as } N \to \infty. \qquad \square$$

Theorem 1.3.1 is a direct consequence of Lemma 1.3.2, Axiom $\mathcal{A}^{\#}$ and:

(1.3.4) LEMMA. *Let $F_1(y) = F_2(y)F_3(y)$, where $F_i(y) = \sum_{n=0}^{\infty} c_i(n)y^n$. Suppose that $F_3(y)$ is absolutely convergent for $|y| < x^{\tau}$ (where $x > 1$ and $\tau > -1$), and that*

$$c_2(N) = BN^u x^N + O(N^v x^{\alpha N}) \text{ as } N \to \infty$$

*(where $\alpha \leq 1$, and $u$, $v$ are non–negative integers). Suppose also that $\alpha < 1$ if $u = 0$, while $u > v$ if $\alpha = 1$. Then, as $N \to \infty$,*

$$c_1(N) = \left[BF_3(x^{-1}) + o(1)\right] N^u x^N.$$

PROOF. It is understood that the numbers, $B$, $u$, $v$, $x$, $\alpha$ are constant relative to $N$. Then the assumption about $c_2(N)$ shows that $F_2(y)$ is absolutely convergent in an open disc with centre the origin, and hence

$$c_1(N) = \sum_{r=0}^{N} c_2(N-r)c_3(r) = \sum_{r=0}^{N} \left\{B(N-r)^u x^{N-r} + O\left((N-r)^v x^{\alpha(N-r)}\right)\right\}c_3(r).$$

In the case when $u = 0$, we have $\alpha < 1$, and so

$$N^v x^{\alpha N} = O(x^{\alpha' N}) \text{ as } N \to \infty,$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

for a suitable constant $\alpha' \geq \alpha$ with $\tau > -\alpha' > -1$. Therefore, in this case,

$$\begin{aligned} c_1(N) &= Bx^N \sum_{r=0}^{N} c_3(r) x^{-r} + O\left(x^{\alpha' N} \sum_{r=0}^{N} |c_3(r)| x^{-\alpha' r}\right) \\ &= Bx^N \left[F_3(x^{-1}) + o(1)\right] + O(x^{\alpha/N}). \end{aligned}$$

Hence the lemma follows when $u = 0$.

When $u > 0$, one can write

$$N^v x^{\alpha N} = O(N^{u-1} x^N) \text{ as } N \to \infty,$$

and therefore

$$\begin{aligned} c_1(N) &= Bx^N \sum_{r=0}^{N} c_3(r) x^{-r} \sum_{i=0}^{u} \binom{u}{i} N^i (-r)^{u-i} + O\left(N^{u-1} x^N \sum_{r=0}^{N} |c_3(r)| x^{-r}\right) \\ &= Bx^N \left[F_3(x^{-1}) + o(1)\right] N^u + O\left(x^N \sum_{i=0}^{u-1} N^i \sum_{r=0}^{N} |c_3(r)| x^{(-1+\epsilon) r}\right) \\ &\quad + O(N^{u-1} x^N), \end{aligned}$$

where $\epsilon > 0$ is arbitrary and may be chosen so that $\tau > -1 + \epsilon$. Hence the lemma follows in this case also, since $F_3(y)$ is absolutely convergent for $|y| < x^\tau$. □

We may now consider some applications of Theorem 1.3.1 to special arithmetical functions of the kinds discussed in [AB], pages 39–40, based on the fact that their associated power series bear simple relationships with the generating function $Z(y)$. The relationships referred to are given in [AB], Theorem 3.3.1, and for the purpose of reference to that theorem it should be emphasized that the coefficients of the series $f^{\#}(y)$ are *here denoted* by $\overline{f}(n)$, *instead of* by $f^{\#}(n) (n = 0, 1, 2, \ldots)$.

First consider the *unitary-divisor* function $d_*$ such that $d_*(a)$ is the total number of divisors $d$ of $a \in \mathcal{G}$ for which $d$ and $a/d$ are coprime. By

[AB], Theorem 3.3.1, $d_*^{\#}(y) = [Z(y)]^2/Z(y^2)$. Since the series for $Z(y^2)$ is absolutely convergent for $|y| < q^{-\frac{1}{2}}$, and $[Z(y)]^{-1} = \mu^{\#}(y)$, where $\mu$ is the *Möbius* function on $\mathcal{G}$, and since $|\overline{\mu}(n)| \leq G(n)$ (see [AB], pages 37, 69), Theorem 1.3.1 therefore implies:

(1.3.5) PROPOSITION. *The average-value of the unitary-divisor function $d_*$ for elements of degree $N$ in $\mathcal{G}$ is asymptotically*

$$AN/Z(q^{-2}) \text{ as } N \to \infty. \quad \square$$

Next consider the point-wise square $d^2$ of the divisor function $d$. By Theorem 3.3.1 of [AB], $d^{2\#}(y) = [Z(y)]^4/Z(y^2)$. Therefore in this case, Theorem 1.3.1 yields:

(1.3.6) PROPOSITION. *The average-value of $d^2(a)$ for elements $a \in \mathcal{G}$ of degree $N$ is asymptotically*

$$A^3N^3/6Z(q^{-2}) \text{ as } N \to \infty. \quad \square$$

In [AB], the function $\beta$ defined as follows was found to have interesting properties: Let $a = p_1^{r_1}p_2^{r_2}\dots p_m^{r_m}$ for distinct primes $p_i \in \mathcal{P}$, and $r_i \geq 1$; then define $\beta(a) = r_1r_2\dots r_m$. Also let $\beta(1) = 1$. Then (see [AB] page 46) $\beta(a)$ can be interpreted as the total number of divisors $d$ of $a$ such that $p^2|d$ whenever a given prime $p|d$. By Theorem 3.3.1 of [AB], $\beta^{\#}(y) = Z(y)Z(y^2)Z(y^3)/Z(y^6)$. Hence Theorem 1.3.1 implies:

(1.3.7) PROPOSITION. *The function $\beta$ has the asymptotic mean-value*

$$Z(q^{-2})Z(q^{-3})/Z(q^{-6}). \quad \square$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Now consider the set $\mathcal{G}_{(k)}$ of all *k–free* elements of $\mathcal{G}$, i.e., elements that are not divisible by any $k$th powers $b^k$ other than 1. By [AB], Theorem 3.3.1, the characteristic function $q_k$ of $\mathcal{G}_{(k)}$ satisfies the relation: $q_k^{\#}(y) = Z(y)/Z(y^k)$. Hence we deduce:

(1.3.8) PROPOSITION. *The set $\mathcal{G}_{(k)}$ of all k–free elements of $\mathcal{G}$ has the asymptotic density $1/Z(q^{-k})$ in $\mathcal{G}(k \geq 2)$.* □

Since $Z(q^{-k}) = \zeta_{\mathcal{G}}(k)$ when $c = q$ is an integer, this last proposition is directly analogous to Proposition 4.4.5 of [AB], which deals with the density of $\mathcal{G}_{(k)}$ subject to Axiom $\mathcal{A}$. In fact, as was mentioned earlier, most of the present results are not only analogous to ones discussed in [AB] Part II, but they often yield *more precise* information than the corresponding conclusions subject to Axiom $\mathcal{A}$; for example, compare Proposition 1.3.6 with the case $k = 2$ of Proposition 4.4.1 in [AB].

## 1.4 Asymptotic Moments of Specific Functions

In addition to studying the average value, it is sometimes of interest to investigate the $k$th **moment** of an arithmetical function $f$ over elements of degree $N$ in $\mathcal{G}$ (i.e., the average value of the point-wise $k$th power $f^k$ for elements of degree $N$), for some number $k \neq 1$. For example, Proposition 1.3.6 gives the asymptotic behaviour of the second moment of $d$ for elements of large degree $N$. If the $k$th moment of $f$ is asymptotically constant, i.e., if $f^k$ has a mean-value $m(f^k)$, we shall refer to $m(f^k)$ as the **asymptotic** $k$th **moment** of $f$.

In order to derive some results about $k$th moments in certain cases, and also for other purposes later on, it is convenient here to first recall a few general concepts, and propositions concerning them, which were discussed in [AB]. These concepts particularly concern certain kinds of arithmetical functions which occur repeatedly in specific number-theoretical problems:

Firstly, an arithmetical function $f$ is called **multiplicative** if and only if $f(1) = 1$ and $f(ab) = f(a)f(b)$ whenever $a$, $b \in \mathcal{G}$ are coprime; $f$ is **completely** multiplicative if and only if $f(1) = 1$ and $f(ab) = f(a)f(b)$ for *all* $a$, $b \in \mathcal{G}$. Secondly, an arithmetical function $f$ is said to be **prime–independent** if an only if, for any prime-power $p^r$, the value $f(p^r)$ is independent of the prime $p \in \mathcal{P}$; a **PIM**-function is one which is both prime-independent and multiplicative. Next, an **additive** function is defined to be a function $g$ on $\mathcal{G}$ such that $g(ab) = g(a) + g(b)$ whenever $a$, $b$ are coprime, and a **completely** additive function $g$ is one such that $g(ab) = g(a) + g(b)$ for *all* $a$, $b \in \mathcal{G}$; $g$ is a **PIA**-function if it is both prime-independent and additive.

It is convenient at this stage to state an important lemma 1.4.1 on

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

multiplicative functions, even though it will not be used directly before Chapter 3 below. This lemma involves *pseudo–convergent* infinite products of formal power series, as treated in [AB], Chapter 2. Strictly speaking, the discussion in [AB] concerns pseudo–convergent products of arithmetical functions relative to a certain non–archimedean metric $\rho$, but by directly analogous arguments one can derive a corresponding theory for formal power series relative to the metric $\sigma$ defined on page 36 of [AB]. Essentially, a pseudo–convergent product is simply a *formal* product, and Lemma 1.4.1 is merely a *translation* of [AB], Corollary 2.4.2, into the context of an additive arithmetical semigroup, similar to the other kinds of translations into this context treated in [AB], Chapter 3. (The lemma does *not* depend on either Axiom $\mathcal{A}^{\#}$ or the assumption that $\partial$ be integer–valued. Its validity for complex values of $y$ in terms of *ordinary* convergence will be discussed in individual instances when this is needed later.)

(1.4.1) Canonical Product Lemma.

*(i)* *If $f$ is a multiplicative function on $\mathcal{G}$ then*

$$f^{\#}(y) = \prod_{p\in\mathcal{P}} \left\{1 + f(p)y^{\partial(p)} + f(p^2)y^{2\partial(p)} + \cdots + f(p^r)y^{r\partial(p)} + \cdots\right\}.$$

*Hence, if $f$ is a PIM-function, then*

$$f^{\#}(y) = \prod_{m>0} \left\{1 + c_1y^m + c_2y^{2m} + \cdots + c_ry^{rm} + \cdots\right\}^{P(m)},$$

*where $c_r = f(p^r)$ $\{p \in \mathcal{P}\}$.*

*(ii)* *If $f$ is a completely multiplicative function on $\mathcal{G}$ then*

$$f^{\#}(y) = \prod_{p\in\mathcal{P}} \left(1 - f(p)y^{\partial(p)}\right)^{-1}.$$

*Hence, if $f$ is both prime–independent and completely multiplicative, then*

$$f^{\#}(y) = \prod_{m>0} (1 - \alpha y^m)^{-P(m)},$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

*where* $\alpha = f(p)$ $\{p \in \mathcal{P}\}$. □

In order to study the various $k$th moments of a given function, and more generally the average values of functions which are not necessarily related by simple finite formulae to $Z(y)$, use can often be made of Lemma 1.4.2 below. This lemma is essentially a re-statement for the present situation of Proposition 4.3.7 and Lemma 4.3.8 of [AB], and may be proved by arguments which are almost identical with those in [AB]:

(1.4.2) LEMMA. *Let* $f$ *denote a PIM–function on* $\mathcal{G}$ *such that* $f(p^r) \neq 0$ *for some prime–power* $p^r \in \mathcal{G}$. *Suppose that* $f(p^r) + O(t^r)$ *as* $r \to \infty$ $(p \in P)$, *for a constant* $t$ *satisfying* $1 < t < q_0^{1/m}$, *where* $q_0 = \min\{|p| : p \in P\}$ *and* $m$ *is the least positive integer such that* $f(p^m) \neq 0$. *Then*

$$f^{\#}(y) = [Z(y^m)]^k g^{\#}(y),$$

*where* $k = f(p^m)$, *and* $g^{\#}(y)$ *is a series which is absolutely convergent when* $|y| < q^{\tau}$ *for some* $\tau > -1/m$. *Further, for* $|y| < q^{\tau}$,

$$g^{\#}(y) = \prod_{p \in \mathcal{P}} \left\{ \sum_{r=0}^{\infty} g(p^r) y^{r\partial(p)} \right\},$$

*where the product is also absolutely convergent.* □

In connection with Lemma 1.4.2, it is worth noting that the above absolutely convergent product decomposition for $|y| < q^{\tau}$ remains valid for any *PIM*–function $g$ such that (for $p \in \mathcal{P}$) *either*

(i) $g(p^r) = 0$ $(0 < r \leq m)$ and $g(p^r) = O(t^r)$ for a constant $t < q_0^{-\tau}$, where $\tau \leq -1/(m+1)$, *or*

(ii) $g(p) \neq 0$ and $g(p^r) = O(t^r)$ for a constant $t < q_0^{-\tau}$, where $\tau \leq -1$; compare Lemma 4.3.8 of [AB]. (The remark at the top of [AB], page 100, regarding another generalization, may also be noted.)

The following applications of Lemma 1.4.2 and Theorem 1.3.1 yield conclusions analogous to but more precise than the corresponding ones which appeared in [AB], Chapter 4, §4, on the basis of Axiom $\mathcal{A}$:

(1.4.3) PROPOSITION. *For $k = 1, 2, \ldots$, there exist constants $B_k$, $B_k^*$ such that the kth moments for elements of degree $N$ of the divisor function $d$ and the unitary-divisor function $d_*$ are respectively asymptotic to $B_k N^{2^k-1}$ and $B_k^* N^{2^k-1}$, as $N \to \infty$.*

PROOF. Some special cases of this proposition were considered already in the previous section. In general, we note (as in [AB], pages 100, 102) that $d^k$, $d_*^k$ are *PIM*-functions such that $d^k(p^r) = (r+1)^k$, $d_*^k(p^r) = 2^k$, for any prime-power $p^r \in \mathcal{G}$. Thus $d^k$, $d_*^k$ satisfy the hypothesis of Lemma 1.4.2, and so

$$d^{k\#}(y) = [Z(y)]^{2^k} g_k^{\#}(y), \; d_*^{k\#}(y) = [Z(y)]^{2^k} h_k^{\#}(y)$$

for certain suitably convergent series $g_k^{\#}(y)$, $h_k^{\#}(y)$. Thus the stated conclusions follow from Theorem 3.1. □

The next proposition seems intuitively to be expected in view of Proposition 1.4.3. However such intuition needs to be treated carefully, since (just as in the parallel situation discussed in [AB], pages 102, 103) one can for example verify that the stated mean-value of $d/d_*$ *differs* from the "expected" number $Z(q^{-2}) = B_1/B_1^*$.

(1.4.4) PROPOSITION. *For $k = 1, 2, \ldots$, the point-wise quotients $d/d_*$ and $d_*/d$ possess the asymptotic kth moments*

$$\begin{aligned} m((d/d_*)^k) &= \prod_{p \in \mathcal{P}} \left\{ 1 + 2^{-k} \sum_{r=2}^{\infty} [(r+1)^k - r^k] q^{-r\partial(p)} \right\}, \\ m(d_*/d)^k) &= \prod_{p \in \mathcal{P}} \left\{ 1 + 2^{k} \sum_{r=2}^{\infty} [(r+1)^{-k} - r^{-k}] q^{-r\partial(p)} \right\}. \end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Proof. Since $d$, $d_*$ are *PIM*–functions taking the values on prime–powers listed earlier, Lemma 1.4.2 can be applied to $f_1 = (d/d_*)^k$ and $f_2 = (d_*/d)^k$ so as to give

$$f_1^{\#}(y) = Z_G(y) F_1^{\#}(y), \ f_2^{\#}(y) = Z_G(y) F_2^{\#}(y)$$

for certain suitably convergent series $F_i^{\#}(y)$. Further (as in [AB], page 103), $\widehat{F}_i = (1-t)\widehat{f}_i$, where for a given *PIM*–function $f$

$$\widehat{f} = \sum_{r=0}^{\infty} f(p^r) t^r.$$

It therefore follows from Theorem 1.3.1 and Lemma 1.4.2 that $f_i$ has the mean–value $F_i(q^{-1})$, and that $F_i(q^{-1})$ has the stated product decomposition $(i = 1, 2)$. □

In a similar way, one may extend Proposition 1.3.7 to:

(1.4.5) Proposition. *For every $k = 1, 2, \ldots$, the function $\beta$ possesses the asymptotic kth moment*

$$m(\beta^k) = \prod_{p \in \mathcal{P}} \left\{ 1 + \sum_{r=2}^{\infty} [r^k - (r-1)^k] q^{-r\partial(p)} \right\}.$$

Proof. Exercise. □

It seems worth remarking that, in addition to asymptotic moments as above, the functions $d/d_*$, $d_*/d$ and $\beta$ also possess asymptotic *distribution functions*, as defined in [AB], page 145. In fact, *all* the results on distribution functions of prime–independent arithmetical functions discussed in

[AB], Chapter 5, §3, may be carried over to the present context *without change*, if one now substitutes Theorem 1.3.1 and Lemma 1.4.2 for the corresponding results used in [AB] subject to Axiom $\mathcal{A}$. A more detailed and refined development of "probabilistic number theory" for $\mathcal{G}$ is elaborated in Chapters 6, 7 below.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

## 1.5 Error Estimates for Certain Averages

In deriving the general asymptotic conclusion of Theorem 1.3.1 earlier, use was made of Lemma 1.3.2, which gives an asymptotic formula for the average value of the function $d_k$, involving both a dominant term and an estimate for the remainder. Such remainder or error estimates are often useful, and so we shall now prove a theorem which yields information of this kind in a variety of special cases of interest.

(1.5.1) THEOREM. *Let $f$, $g$ be arithmetical functions with the property that*

$$f^{\#}(y) = [Z(y)]^k g^{\#}(y),$$

*where $k$ is a positive integer, and suppose that (for some constant $\tau > -1$)*

$$\overline{g}(N) = O(q^{-\tau N}) \text{ as } N \to \infty.$$

*Then, as $N \to \infty$,*

$$\overline{f}(N) = \frac{A^k}{(k-1)!} g^{\#}(q^{-1}) N^{k-1} q^N + \begin{cases} O(q^{-\tau N}) & \text{if } k = 1,\ \tau < -\nu, \\ O(N q^{\nu N}) & \text{if } k = 1,\ \tau = -\nu, \\ O(q^{\nu N}) & \text{if } k = 1,\ \tau > -\nu, \\ O(N^{k-2} q^N) & \text{if } k \geq 2. \end{cases}$$

PROOF. This theorem is a consequence of Axiom $\mathcal{A}^{\#}$, Lemma 1.3.2 and two further auxiliary conclusions below:

(1.5.2) LEMMA. *Let $F_1(y) = F_2(y)F_3(y)$, where $F_i(y) = \sum_{n=0}^{\infty} c_i(n) y^n$. Suppose that, as $N \to \infty$,*

$$c_2(N) = Bx^N + O(x^{\alpha N}),\ c_3(N) = O(x^{-\tau N}),$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

*where $B$, $x$, $\alpha$, $\tau$ are constants satisfying $x > 1$, $\alpha < 1$, $\tau > -1$. Then, as $N \to \infty$,*

$$c_n(N) = BF_3(x^{-1})x^N + \begin{cases} O(x^{-\tau N}) & \textit{if } \tau < -\alpha, \\ O(Nx^{\alpha N}) & \textit{if } \tau = -\alpha, \\ O(x^{\alpha N}) & \textit{if } \tau > -\alpha. \end{cases}$$

Proof. It follows easily from the above hypothesis that $F_3(y)$ is absolutely convergent for $|y| < x^\tau$, while $F_2(y)$ and $F_1(y)$ are both absolutely convergent for $|y| < x^{-1}$. Further, for $|y| < x^\tau$,

$$\sum_{r=0}^{N} c_3(r)y^r = F_3(y) + O\left(\sum_{r>N} |x^{-\tau}y|^r\right) = F_3(y) + O\left(|x^{-\tau}y|^N\right);$$

in particular,

$$\sum_{r=0}^{N} c_3(r)x^{-r} = F_3(x^{-1}) + O\left(x^{-(1+\tau)N}\right).$$

Then the assumed equation for $F_1(y)$ and the estimate for $c_2(N)$ give

$$\begin{aligned} c_1(N) &= \sum_{r=0}^{N} c_2(N-r)c_3(r) = \sum_{r=0}^{N} \left[Bx^{N-r} + O(x^{\alpha(N-r)})\right] c_3(r) \\ &= Bx^N\left[F_3(x^{-1}) + O(x^{-(1+\tau)N})\right] + O\left(x^{\alpha N}\sum_{r=0}^{N} |c_3(r)|x^{-\alpha r}\right) \\ &= Bx^N F_3(x^{-1}) + O(x^{-\tau N}) + O\left(x^{\alpha N}\sum_{r=0}^{N} x^{-(\tau+\alpha)r}\right). \end{aligned}$$

If $\tau < -\alpha$, the preceding remainder terms reduce to $O(x^{-\tau N}) + O(x^{-\alpha N}x^{-(\tau+\alpha)N}) = O(x^{-\tau N})$; if $\tau = -\alpha$, they become $O(x^{-\tau N}) + O(Nx^{\alpha N}) = O(Nx^{\alpha N})$; lastly if $\tau > -\alpha$, convergence of the geometric series implies that the remainder is $O(x^{-\tau N}) + O(x^{\alpha N}) = O(x^{\alpha N})$. This proves the lemma. □

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Lemma 1.5.2 covers the case $k = 1$ of Theorem 1.5.1. For the general case, consider:

(1.5.3) LEMMA. *Let $F_1(y) = F_2(y)F_3(y)$, where $F_i(y) = \sum_{n=0}^{\infty} c_i(n)y^n$. Suppose that (as $N \to \infty$)*

$$c_2(N) = BN^u x^N + O(N^{u-1}x^N),\ c_3(N) = O(x^{-\tau N}),$$

*where $B$, $u$, $x$, $\tau$ are constants such that $x > 1$, $\tau > -1$, and $u$ is a positive integer. Then as $N \to \infty$*

$$c_1(N) = BF_3(x^{-1})N^u x^N + O(N^{u-1}x^N).$$

PROOF. As in the proof of Lemma 1.3.4,

$$\begin{aligned} c_1(N) &= Bx^N \sum_{r=0}^{N} c_3(r)x^{-r} \sum_{i=0}^{u} \binom{u}{i} N^i(-r)^{u-i} \\ &\quad + O\left(N^{u-1}x^N \sum_{r=0}^{N} |c_3(r)|x^{-r}\right) \\ &= BN^u x^N \sum_{r=0}^{N} c_3(r)x^{-r} + O\left(x^N \sum_{i=0}^{u-1} N^i \sum_{r=0}^{N} |c_3(r)|x^{(-1+\epsilon)r}\right) \\ &\quad + O(N^{u-1}x^N), \end{aligned}$$

where $\epsilon > 0$ is arbitrary and may be chosen so that $\tau > -1 + \epsilon$. In the present situation, the estimate for $\sum_{r=0}^{N} c_3(r)x^{-r}$ which occurred in the proof of Lemma 1.5.2, and the absolute convergence of $F_3(y)$ for $|y| < x^{\tau}$, imply that

$$c_1(N) = BN^u x^N \left[F_3(x^{-1}) + O(x^{-(1+\tau)N})\right] + O(N^{u-1}x^N).$$

Therefore Lemma 1.5.3 follows. □

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

In the first place, Theorem 1.5.1 may be used to refine some of the conclusions relating to average values of special arithmetical functions that were discussed in Section 1.3.

(1.5.4) PROPOSITION. *The average value of the unitary-divisor function $d_*$ for elements of degree $N$ in $\mathcal{G}$ is*

$$A[Z(q^{-2})]^{-1}N + O(1) \text{ as } N \to \infty.$$

PROOF. The proof of Proposition 3.5 shows that $d_*^{\#}(y) = [Z(y)]^2 g^{\#}(y)$, where $g^{\#}(y) = \mu^{\#}(y^2) = \sum_{n=0}^{\infty} \overline{\mu}(n) y^{2n}$. Since $|\overline{\mu}(n)| \leq G^{\#}(n)$, Axiom $\mathcal{A}^{\#}$ then implies that $\overline{g}(N) = O(q^{\frac{1}{2}N})$ as $N \to \infty$. Hence the present proposition follows from Theorem 1.5.1. □

The next proposition follows in a similar way from Theorem 1.5.1 and the equation $d^{2\#}(y) = [Z(y)]^4/Z(y^2)$.

(1.5.5) PROPOSITION. *The average value of $d^2(a)$ for elements $a \in \mathcal{G}$ of degree $N$ is*

$$\frac{1}{6}A^3[Z(q^{-2})]^{-1}N^3 + O(N^2) \text{ as } N \to \infty. \qquad \square$$

For the function $\beta$, we now obtain the improved conclusion:

(1.5.6) PROPOSITION. *The average value of $\beta$ for elements of degree $N$ in $\mathcal{G}$ is*

$$Z(q^{-2})Z(q^{-3})[Z(q^{-6})]^{-1} + \begin{cases} O(q^{-\frac{1}{2}N}) & \text{if } \nu < \frac{1}{2}, \\ O(Nq^{-\frac{1}{2}N}) & \text{if } \nu = \frac{1}{2}, \\ O(q^{(\nu-1)N}) & \text{if } \nu > \frac{1}{2}. \end{cases}$$

Proof. We have $\beta^{\#}(y) = Z(y)g^{\#}(y)$, where $g^{\#}(y) = Z(y^2)Z(y^3)/Z(y^6)$. Then $g^{\#}(y) = Z(y^2)h^{\#}(y)$, where $h^{\#}(y) = Z(y^3)/Z(y^6)$ is absolutely convergent for $|y| < q^{-\frac{1}{3}}$. Hence

$$\begin{aligned}\overline{g}(N) &= \sum_{0\leq r\leq\frac{1}{2}N} G(r)\overline{h}(N-2r) = O\left(\sum_{0\leq r\leq\frac{1}{2}N} q^r|\overline{h}(N-2r)|\right)\\ &= O\left(q^{\frac{1}{2}N}\sum_{0\leq r\leq\frac{1}{2}N}|\overline{h}(N-2r)|q^{-\frac{1}{2}(N-2r)}\right) = O(q^{\frac{1}{2}N}),\end{aligned}$$

since $h^{\#}(q^{-\frac{1}{2}})$ is absolutely convergent. Hence Theorem 1.5.1 may be applied with $k=1$ and $\tau = -\frac{1}{2}$. □

If $\chi_E$ denotes the characteristic function of a given subset $E$ of $\mathcal{G}$, it is reasonable to describe the average value of $\chi_E$ for elements of degree $N$ in $\mathcal{G}$ as the **density** of $E$ **relative to** elements of degree $N$. By appealing to the equation $q_k^{\#}(y) = Z(y)/Z(y^k)$, the following refinement of Proposition 1.3.8 (phrased in the preceding terminology) may be deduced:

(1.5.7) Proposition. *For $k \geq 2$, the density of the set $\mathcal{G}_{(k)}$ of all $k$-free elements in $\mathcal{G}$ relative to the elements of degree $N$ is*

$$[Z(q^{-k})]^{-1} + \begin{cases} O(q^{N(1-k)/k}) & \text{if } \nu < 1/k,\\ O(Nq^{N(1-k)/k}) & \text{if } \nu = 1/k,\\ O(q^{(\nu-1)N}) & \text{if } \nu > 1/k.\end{cases} \qquad \square$$

In the next section, Lemma 1.5.2 will be applied to the asymptotic enumeration of finite modules and semisimple algebras over the ring of integral

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

functions in an algebraic function field over $F$, and in particular this will lead to the verification of Axiom $\mathcal{A}^{\#}$ for the categories $\mathcal{F}_q$ and $\mathcal{S}_q$ discussed in Section 1.1. Before turning to this, however, it may be of interest to first consider some questions relating to arithmetical functions of the *Euler* and *divisor–sum* types:

In the present context of an additive arithmetical semigroup $\mathcal{G}$ satisfying Axiom $\mathcal{A}^{\#}$, one "Euler–type" function of special interest is the function $\phi_*$ on $\mathcal{G}$ such that $\phi_*(a)$ is the total number of elements of the *same* degree as $a$ that are coprime to $a$ in $\mathcal{G}$; also, the "divisor–sum" function of greatest relevance here seems to be the function $\sigma_*$ such that $\sigma_*(a) = \sum_{d|a} \partial(d)$.

(1.5.8) PROPOSITION.

*(i) The average value of $\phi_*$ for elements of degree $N$ is*

$$A[Z(q^{-2}]^{-1}q^N + \begin{cases} O(N) & \text{if } \nu = 0, \\ O(q^{\nu N}) & \text{if } \nu > 0. \end{cases}$$

*(ii) The average value of $\sigma_*$ for elements of degree $N$ is*

$$\frac{1}{2}AN^2 + O(N).$$

PROOF. First consider the following lemma, which *does not* depend on Axiom $\mathcal{A}^{\#}$:

(1.5.9) LEMMA.

*(i)* $\phi_*^{\#}(y) = \left(\sum_{n=0}^{\infty} [G(n)]^2 y^n\right) / Z_G(y)$.

*(ii)* $\sigma_*^{\#}(y) = Z(y) \left\{\sum_{n=0}^{\infty} nG(n) y^n\right\}$.

PROOF. By [AB], Corollary 2.5.3, the Möbius function $\mu$ on $\mathcal{G}$ has the property that $\sum_{d|a} \mu(d) = 0$ for $1 \neq a \in \mathcal{G}$; also, the last sum is trivially equal to 1 for $a = 1$. Therefore, if $(b, a)$ denotes the *g.c.d.* of $b$ and $a$ in $\mathcal{G}$, then

$$\begin{aligned}
\phi_*(a) &= \sum_{\partial(b)=\partial(a),(b,a)=1} 1 = \sum_{\partial(b)=\partial(a)} \sum_{d|(b,a)} \mu(d) \\
&= \sum_{d|a} \mu(d) \sum_{d|b,\partial(b)=\partial(a)} 1 = \sum_{d|a} \mu(d) G\left(\partial\left(\frac{a}{d}\right)\right).
\end{aligned}$$

Hence

$$\begin{aligned}
\overline{\phi_*}(n) &= \sum_{\partial(a)=n} \phi_*(a) = \sum_{\partial(a)=n} \sum_{d|a} \mu(d) G\left(\partial\left(\frac{a}{d}\right)\right) \\
&= \sum_{\partial(cd)=n} \mu(d) G(\partial(c)) = \sum_{i+j=n} \sum_{\partial(c)=i} \sum_{\partial(d)=j} \mu(d) G(\partial(c)) \\
&= \sum_{i+j=n} [G(i)]^2 \overline{\mu}(j).
\end{aligned}$$

Since $\mu^{\#}(y) = 1/Z(y)$, the formula for $\phi_*^{\#}(y)$ follows.

In the case of $\sigma_*$, its definition gives

$$\begin{aligned}
\overline{\sigma_*}(n) &= \sum_{\partial(a)=n} \sigma_*(a) = \sum_{\partial(a)=n} \sum_{cd=a} \partial(d) = \sum_{i+j=n} \sum_{\partial(c)=i} \sum_{\partial(d)=j} j \\
&= \sum_{i+j=n} G(i)G(j)j.
\end{aligned}$$

This implies the stated formula for $\sigma_*^{\#}(y)$. □

It now follows that

$$\begin{aligned}
\overline{\phi_*}(N) &= \sum_{r=0}^{N} [G(N-r)]^2 \overline{\mu}(r) = \sum_{r=0}^{N} \left[Aq^{N-r} + O(q^{\nu(N-r)})\right]^2 \overline{\mu}(r) \\
&= A^2 q^{2N} \sum_{r=0}^{N} \overline{\mu}(r) q^{-2r} + O\left(q^{(1+\nu)N} \sum_{r=0}^{N} |\overline{\mu}(r)| q^{-(1+\nu)r}\right)
\end{aligned}$$

$$\begin{aligned} &= A^2q^{2N}\left[\mu^{\#}(q^{-2}) + O\left(\sum_{r>N} q^{-r}\right)\right] + O\left(q^{(1+\nu)N}\sum_{r=0}^{N} q^{-\nu r}\right) \\ &= A^2q^{2N}\mu^{\#}(q^{-2}) + O(q^N) + \begin{cases} O(Nq^N) & \text{if } \nu = 0, \\ O(q^{(1+\nu)N}) & \text{if } \nu > 0. \end{cases} \end{aligned}$$

This proves the assertion of Proposition 1.5.8 about the average value of $\phi_*$.

In the case of $\sigma_*$, we have

$$\begin{aligned} \overline{\sigma_*}(N) &= \sum_{r=0}^{N} G(N-r)rG(r) = \sum_{r=0}^{N}\left[Aq^{N-r} + O(q^{\nu(N-r)})\right] r\left[Aq^r + O(q^{\nu r})\right] \\ &= A^2q^n\sum_{r=0}^{N} r + O\left(\sum_{r=0}^{N} r\left[q^{N+r(\nu-1)} + q^{\nu N+r(1-\nu)} + q^{\nu N}\right]\right) \\ &= \frac{1}{2}A^2N^2q^N + O(Nq^N). \end{aligned}$$

This implies the second assertion of Proposition 5.8. □

(1.5.10) Corollary. *The set of all ordered pairs of coprime elements of the same degree possesses the asymptotic density* $[Z(q^{-2})]^{-1}$ *within the set of all ordered pairs of elements of the same degree in* $\mathcal{G}$.

Proof. There are $[G(N)]^2 \sim A^2q^{2N}$ ordered pairs of elements of degree $N$ in $\mathcal{G}$, and $\overline{\phi_*}(N) \sim A^2[Z(q^{-2})]^{-1}q^{2N}$ pairs of coprime elements of this degree. Hence, in an obvious sense, the stated "asymptotic density" exists. □

The above corollary confines attention to pairs of elements of the *same* degree. In order to deal with arbitrary ordered pairs, one may instead make use of the "Euler" function $\phi$ defined in [AB], page 40, which has the property that $\phi(a)$ is the total number of elements $b$ such that $b$ is coprime to $a$ and $\partial(b) \leq \partial(a)$. By Theorem 3.3.1 of [AB], if $N_G^{\#}(n) = \sum_{r\leq n} G(r)$,

then

$$\phi^{\#}(y) = \left( \sum_{n=0}^{\infty} G(n) N_G^{\#}(n) y^n \right) \Big/ Z(y).$$

Bearing this in mind, the reader may perhaps like to verify the conclusion of the following lemma, as an exercise.

(1.5.11) LEMMA. *The average value of $\phi$ for elements of degree $N$ is*

$$\frac{q}{q-1} A[Z(q^{-2})]^{-1} q^N + \begin{cases} O(N^2) & \textit{if } \nu = 0, \\ O(q^{\nu N}) & \textit{if } \nu > 0. \end{cases} \qquad \square$$

With the aid of this lemma, we now prove:

(1.5.12) PROPOSITION. *The set of all ordered pairs of coprime elements of $\mathcal{G}$ possesses the asymptotic density $[Z(q^{-2})]^{-1}$ within the set of all ordered pairs of elements of $\mathcal{G}$.*

PROOF. Asymptotically, as $N \to \infty$, there are $\left[\frac{q}{q-1} A q^N\right]^2$ ordered pairs $a$, $b \in \mathcal{G}$ with $\partial(a) \leq N$, $\partial(b) \leq N$. Also, as in [AB], page 248, it may be noted that the total number $\Delta(N)$ of ordered pairs of coprime elements $a$, $b \in \mathcal{G}$ with $\partial(a) \leq N$, $\partial(b) \leq N$ is given by

$$\begin{aligned}
\Delta(N) &= \sum_{\partial(a) \leq N} \; \sum_{\partial(a) \leq N, (b,a)=1} 1 \\
&= \sum_{\partial(a) \leq N} \; \sum_{\partial(b) \leq \partial(a), (b,a)=1} 1 + \sum_{\partial(a) \leq N} \; \sum_{\substack{\partial(b) \leq N \\ \partial(b) > \partial(a), (b,a)=1}} 1 \\
&= 2 \sum_{\partial(a) \leq N} \phi(a) - \sum_{\partial(a) \leq N} \; \sum_{\partial(b) = \partial(a), (b,a)=1} 1 \\
&= 2 \sum_{n \leq N} \overline{\phi}(n) - \sum_{n \leq N} \overline{\phi_*}(n).
\end{aligned}$$

Therefore, by Proposition 1.5.8 and Lemma 1.5.11, as $N \to \infty$,

$$\begin{aligned}\Delta(n) &\sim 2\frac{q}{a-1}A^2[Z(q^{-2})]^{-1}\frac{q^{2N+2}}{q^2-1} - A^2[Z(q^{-2})]^{-1}\frac{q^{2N+2}}{q^2-1} \\ &= A^2[Z(q^{-2})]^{-1}q^{2N}\frac{q^2}{q^2-1}\left[2\frac{q}{q-1}-1\right] = \left[\frac{q}{q-1}Aq^N\right]^2[Z(q^{-2})]^{-1}.\end{aligned}$$

Hence, in an obvious sense once more, one obtains the stated "asymptotic density" $[Z(q^{-2})]^{-1}$. □

By way of illustration, it may be noted that for the semigroup $\mathcal{G}_q$ of all monic polynomials over $\mathbb{F}_q$ the above results imply that the asymptotic density of the coprime pairs of polynomials is $1 - q^{-1}$. Similarly, the next proposition implies that for coprime $k$–tuples of polynomials in $\mathcal{G}_q$ the corresponding asymptotic density is $1 - q^{1-k}$.

(1.5.13) PROPOSITION. *The set of all coprime ordered $k$–tuples of elements of $\mathcal{G}$ possesses the asymptotic density $[Z(q^{-k})]^{-1}$ within the set of all ordered $k$–tuples of elements of $\mathcal{G}$, where $k \geq 2$.*

PROOF. The following argument provides an alternative proof of Proposition 1.5.12, in the special case when $k = 2$: Firstly, note that (as $N \to \infty$) there are asymptotically $\left[\frac{q}{q-1}Aq^N\right]^k$ ordered $k$–tuples $a_1, \ldots, a_k \in G$ with $\partial(a_i) \leq N$. Let $\Delta_k(N)$ denote the total number of these $k$–tuples which are *coprime*, i.e., for which the g.c.d. of $a_1, \ldots, a_k$ is 1. Then, by a simple re–wording of Lemma 4.5.13 of [AB],

$$\Delta_k(N) = \sum_{\partial(a)\leq N} \mu(a)\left\{\sum_{n\leq N-\partial(a)} G(n)\right\}^k,$$

where $\mu$ is the Möbius function on $\mathcal{G}$. Therefore, if $B = \frac{q}{q-1}A$ and $\nu > 0$,

$$\Delta_k(N) = \sum_{r\leq N} \overline{\mu}(r)\left[Bq^{N-r} + O(q^{\nu(N-r)})\right]^k$$

$$\begin{aligned}
&= \sum_{r\le N} \overline{\mu}(r)\left[B^k q^{(N-r)k} + O(q^{(N-r)(k-1+\nu)})\right] \\
&= B^k q^{Nk} \sum_{r\le N} \overline{\mu}(r) q^{-kr} + O\left(q^{N(k-1+\nu)} \sum_{r\le N} |\overline{\mu}(r)| q^{-r(K-1+\nu)}\right) \\
&= B^k q^{Nk} \left\{\mu^{\#}(q^{-k}) + O\left(\sum_{r>N} |\overline{\mu}(r)| q^{-kr}\right)\right\} \\
&\quad + O\left(q^{N(k-1+\nu)} \sum_{r\le N} q^{(2-k-\nu)r}\right) \\
&= B^k q^{Nk} \left\{\mu^{\#}(q^{-k}) + O\left(\sum_{r\le N} q^{(1-k)r}\right)\right\} + O(q^{N(k-1+\nu)}) \\
&= B^k q^{Nk} \mu^{\#}(q^{-k}) + O(q^{N(k-1+\nu)}).
\end{aligned}$$

Similarly, if $\nu = 0$, one obtains

$$\Delta_k(N) = B^k q^{Nk} \mu^{\#}(q^{-k}) + \begin{cases} O(N^2 q^{N(k-1)}) & \text{if } k = 2, \\ O(N q^{N(k-1)} & \text{if } k > 2. \end{cases}$$

In an obvious sense yet again, it follows that the stated "asymptotic density" exists. □

(1.5.14) Corollary. *As $N \to \infty$, the total number $\Delta_k(N)$ of coprime ordered $k$-tuples $a_1, \ldots, a_k \in G$ with $\partial(a_i) \le N$ is equal to*

$$\left[\frac{q}{q-1} A q^N\right]^k [Z(q^{-k})]^{-1} + \begin{cases} O(N^2 q^{N(k-1)}) & \textit{if } k = 2,\ \nu = 0, \\ O(N q^{N(k-1)}) & \textit{if } k > 2,\ \nu = 0, \\ O(q^{N(k-1+\nu)}) & \textit{if } \nu > 0. \end{cases} \qquad \square$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

# CHAPTER 2

# ASYMPTOTIC ENUMERATION AND MORE REFINED ESTIMATES

## 2.1 Asymptotic Enumeration of Modules and Algebras

Consider the category $\mathcal{F}_q$ of all (unital) modules of finite cardinal over the Galois polynomial ring $\mathbb{F}_q[X]$, which was discussed under Example 1.1.2 of Section 1.1. This is a special case of the category $\mathcal{F}_D$ of Example 1.1.6 in Section 1.1 but, since our treatment of the latter category uses facts about it which may be less familiar to some readers, we begin with a *direct* discussion of $\mathcal{F}_q$ alone.

(2.1.1) THEOREM. *The total number $\mathcal{F}_q(N)$ of non-isomorphic modules of cardinal $q^N$ in $\mathcal{F}_q$ is equal to*

$$P_0(q^{-1})q^N + O\left(q^{\frac{1}{2}N}\right) \ \textit{as}\ N \to \infty,$$

*where $P_0(y) = \prod_{r=1}^{\infty}(1-y^r)^{-1}$ is the classical "partition" generating function.*

PROOF. Following the general pattern of discussion in Chapter 3, §2, of [AB], we see from the earlier description of the "primes" (i.e., indecompos-

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

able modules) in $\mathcal{F}_q$ that $\mathcal{F}_q$ has the generating function

$$\begin{aligned}
Z_{\mathcal{F}_q}(y) &= \sum_{n=0}^{\infty} \mathcal{F}_q(n) y^n \\
&= \prod \left\{ \left(1 - y^{r\partial(p)}\right)^{-1} : r \geq 1, \text{ monic prime polynomials } p \in GF[q,t] \right\} \\
&= \prod_{r=1}^{\infty} \prod \left\{ \left(1 - y^{r\partial(p)}\right)^{-1} : \text{ monic prime polynomials } p \right\} \\
&= \prod_{r=1}^{\infty} Z_q(y^r),
\end{aligned}$$

where

$$Z_q(y) = \prod \left\{ \left(1 - y^{\partial(p)}\right)^{-1} : \text{ monic prime polynomials } p \in \mathbb{F}_q[X] \right\}$$

is the generating function of the semigroup $\mathcal{G}_q$. Since

$$Z_q(y) = \sum_{n=0}^{\infty} q^n y^n = (1 - qy)^{-1},$$

by Example 1.1.1 (see also [AB], page 60), it follows that

$$Z_{\mathcal{F}_q}(y) = \prod_{r=1}^{\infty} (1 - qy^r)^{-1}.$$

Now let $F_m(y) = \prod_{r=m}^{\infty}(1 - qy^r)^{-1}$. For $r \geq m \geq 1$ and $|y| \leq \rho < q^{-1/r}$,

$$\left|(1 - qy^r)^{-1} - 1\right| \leq \sum_{n=1}^{\infty} |qy^r|^n \leq \frac{q|y|^r}{1 - q\rho^r} \leq \frac{q|y|^r}{1 - q\rho^m};$$

therefore $\sum_{r=m}^{\infty} \left|(1 - qy^r)^{-1} - 1\right|$ converges uniformly for $|y| \leq \rho < q^{-1/m}$. By standard theorems on infinite products of analytic functions (see for example Knopp [1], §57), it follows that $F_m(y)$ is an analytic function of $y$ in the disc $|y| < q^{-1/m}$, and that its Taylor expansion about the origin may be calculated by formal multiplication of the series for $(1 - qy^r)^{-1}$ $[r \geq m]$.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Hence, if $F_2(y) = \sum_{n=0}^{\infty} a_n y^n$, $F_3(y) = \sum_{n=0}^{\infty} b_n y^n$,

$$\begin{aligned} |a_N| &= \left| \sum_{0 \le r \le \frac{1}{2}N} q^r b_{N-2r} \right| \le q^{\frac{1}{2}N} \sum_{0 \le r \le \frac{1}{2}N} |b_{N-2r}| q^{-\frac{1}{2}(N-2r)} \\ &= O(q^{\frac{1}{2}N}), \end{aligned}$$

since $F_3(q^{-\frac{1}{2}})$ is absolutely convergent. Since $Z_{\mathcal{F}_q}(y) = (1-qy)^{-1}F_2(y)$, Lemma 1.5.2 may now be applied, with $B = 1$, $x = q$, $\alpha = 0$ and $\tau = -\frac{1}{2}$. This yields the conclusion:

$$\mathcal{F}_q(N) = F_2(q^{-1})q^N + O(q^{\frac{1}{2}N}) = P_0(q^{-1})q^N + O(q^{\frac{1}{2}N}),$$

as $N \to \infty$, with $P_0(y) = \prod_{r=1}^{\infty}(1-y^r)^{-1}$. □

(2.1.2) COROLLARY. *The associated additive arithmetical semigroup of $\mathcal{F}_q$ satisfies Axiom $\mathcal{A}^{\#}$.* □

The analogue of Theorem 2.1.1 for the category $\mathcal{S}_q$ of Example 1.1.3 in Section 1.1 is:

(2.1.3) THEOREM. *The total number $\mathcal{S}_q(N)$ of non–isomorphic semi–simple $\mathbb{F}_q[X]$–algebras of cardinal $q^N$ is equal to*

$$A_q q^N + O(q^{\frac{1}{2}N}) \text{ as } N \to \infty,$$

*where* $A_q = \prod_{rm^2>1}(1-q^{1-rm^2})^{-1}$.

PROOF. From the earlier discussion of Example 1.1.3, and similarly to the treatment of Example 3.2.5 in [AB], one sees that the Euler product formula for the generating function of the category $\mathcal{S}_q$ yields:

$$Z_{\mathcal{S}_q}(y) = \sum_{n=0}^{\infty} \mathcal{S}_q(n)y^n$$

$$
\begin{aligned}
&= \prod\Big\{ \left(1-y^{rm^2\partial(p)}\right)^{-1} : r \geq 1,\ m \geq 1, \text{ monic prime polynomials} \\
&\qquad\qquad p \in \mathbb{F}_q[X]\Big\} \\
&= \prod_{r,m\geq 1} \prod\Big\{ \left(1-y^{rm^2\partial(p)}\right)^{-1} : \text{ monic prime polynomials } p\Big\} \\
&= \prod_{r,m\geq 1} Z_q(y^{rm^2}),
\end{aligned}
$$

where $Z_q(y)$ again denotes the generating function of $\mathcal{G}_q$.

Consider the product $H(y) = \prod_{r=1}^{\infty} \prod_{m=2}^{\infty} \left(1 - qy^{rm^2}\right)^{-1}$. As in the proof of Theorem 6.1, for $|y| \leq \rho < q^{-\frac{1}{4}}$,

$$
\begin{aligned}
\sum_{r=1}^{\infty} \sum_{m=2}^{\infty} \left|\left(1-qy^{rm^2}\right)^{-1}\right| &\leq \frac{q}{1-q\rho^4} \sum_{r=1}^{\infty} \sum_{m=2}^{\infty} |y|^{rm^2} \\
&= \frac{q}{1-q\rho^4} \sum_{m=2}^{\infty} \frac{|y|^{m^2}}{1-|y|^{m^2}},
\end{aligned}
$$

where the last ("Lambert") series is uniformly convergent; compare Knopp [1], §58. Hence, as in the discussion of $F_m(y)$ in the proof of Theorem 2.1.1, it may be deduced that the power series in $y$ for $H(y)$ converges absolutely when $|y| < q^{-\frac{1}{4}}$. Thus the power series for $F_3(y)H(y)$ converges absolutely when $|y| < q^{-\frac{1}{3}}$.

Now, similarly to the proof of Theorem 2.1.1, write $Z_{\mathcal{S}_q}(y) = (1 - qy)^{-1}F_2^*(y)$, where $F_2^* = F_2(y)H(y) = \sum_{n=0}^{\infty} a_n^* y^n$, and verify that $a_N^* = O(q^{\frac{1}{2}N})$ as $N \to \infty$. The present theorem then also follows from Lemma 1.5.2. □

(2.1.4) Corollary. *The associated additive arithmetical semigroup of $\mathcal{S}_q$ satisfies Axiom $\mathcal{A}^{\#}$.* □

The extension of Theorems 2.1.1 and 2.1.3 to the categories $\mathcal{F}_D$, $\mathcal{S}_D$ of Examples 1.1.6 and 1.1.7 of Section 1.1 is quite straight-forward if one assumes the facts about these categories and about algebraic function fields which were quoted in Section 1.1:

(2.1.5) THEOREM. *Let $\mathcal{F} = \mathcal{F}_D$ denote the category of all (unital) $D$–modules of finite cardinal, where $D$ is the ring of integral functions in an algebraic function field in one variable over $\mathbb{F}_q$. Then the total number $\mathcal{F}(N)$ of non–isomorphic modules of cardinal $q^N$ in $\mathcal{F}$ is equal to*

$$A_{\mathcal{F}}q^N + O\left(q^{\frac{1}{2}N}\right) \text{ as } N \to \infty,$$

*where $A_{\mathcal{F}} = A_D \prod_{r=2}^{\infty} \zeta_D(r)$, and $A_D$ is the constant described in Example 1.1.5.*

PROOF. The ring $D$ is assumed to be as described in Example 1.1.5. Then the earlier description of the indecomposable modules in $\mathcal{F}$ implies that

$$\begin{aligned} Z_{\mathcal{F}}(y) &= \prod\left\{\left(1 - y^{r\partial(\rho)}\right)^{-1} : r \geq 1, \text{ prime ideals } \rho \text{ in } D\right\} \\ &= \prod_{r=1}^{\infty} Z_D(y^r), \end{aligned}$$

where $\partial(\alpha) = \log_q N(\alpha)$ denotes the degree of an ideal $\alpha$ in $D$, and $Z_D(y)$ is the generating function of the semigroup $\mathcal{G}_D$. Then

$$Z_D(y) = \sum_{n=0}^{\infty} D(n)y^n = \frac{P(y)}{1 - qy},$$

where $Q(y)$ is the result of substituting $y$ for $q^{-z}$ in

$$Q(q^{-z}) = \zeta_D(z)(1 - q^{1-z}).$$

Since $D(n) = A_D q^n + O(1)$, where $A_D = Q(q^{-1})$, there exists a positive constant $C$ such that $D(n) \leq Cq^n$ for $n \geq 0$.

Continuing with the pattern of the proof of Theorem 2.1.1, we now note that (for $r \geq m \geq 1$ and $|y| \leq \rho < q^{-1/r}$)

$$|Z_D(y^r) - 1| \leq C \sum_{n=1}^{\infty} q^n |y|^{rn} \leq \frac{Cq|y|^r}{1 - q\rho^m}.$$

Therefore $\sum_{r=m}^{\infty} |Z_D(y^r) - 1|$ converges uniformly for $|y| \leq \rho < q^{-1/m}$, and so in the present general case the product $F_m(y) = \prod_{r=m}^{\infty} Z_D(y^r)$ also defines an analytic function of $y$ in the disc $|y| < q^{-1/m}$, whose Taylor expansion may be calculated by formal multiplication of the series for $Z_D(y^r)\,[r \geq m]$. The rest of the proof of Theorem 2.1.1 carries over without change, except that one must now use the estimate $D(r) = O(q^r)$, and substitute $B = A_D$ in Lemma 1.5.2. This yields:

$$\mathcal{F}(N) = A_{\mathcal{F}} q^N + O\left(q^{\frac{1}{2}N}\right) \text{ as } N \to \infty,$$

where

$$A_{\mathcal{F}} = A_D F_2(q^{-1}) = A_D \prod_{r=2}^{\infty} Z_D(q^{-r}) = A_D \prod_{r=2}^{\infty} \zeta_D(r). \qquad \square$$

(2.1.6) Corollary. *The associated additive arithmetical semigroup of the category $\mathcal{F}_D$ satisfies Axiom $\mathcal{A}^{\#}$.* □

It is interesting to observe the close parallel between Theorem 2.1.5 and Theorem 5.1.1 in [AB], which concerns finite modules over the ring of all algebraic integers in an algebraic *number* field. In particular, Theorem 2.1.1 regarding the polynomial ring counterpart $\mathcal{F}_q$ of the category of all ordinary *finite abelian groups*, corresponds to a theorem of Erdős and Szekeres given as Corollary 5.1.2 in [AB]. Similarly, Theorem 2.1.3 is a close analogue of Theorem 5.1.7 in [AB], which covers the category of all *semisimple finite rings*, while the following theorem is analogous to one concerning semisimple finite algebras over a ring of algebraic *integers* (see J. Knopfmacher [1]):

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

(2.1.7) THEOREM. *Let $\mathcal{S} = \mathcal{S}_D$ denote the category of all semi–simple finite algebras over the ring $D$ of integral functions in an algebraic function field in one variable over $\mathbb{F}_q$. Then the total number $\mathcal{S}(N)$ of non–isomorphic algebras of cardinal $q^N$ in $\mathcal{S}$ is equal to*

$$A_{\mathcal{S}} q^N + O\left(q^{\frac{1}{2}N}\right) \text{ as } N \to \infty,$$

*where $A_{\mathcal{S}} = A_D \prod_{rm^2>1} \zeta_D(rm^2)$.*

PROOF. Exercise. □

(2.1.8) COROLLARY. *The associated additive arithmetical semigroup of the category $\mathcal{S}_D$ satisfies Axiom $\mathcal{A}^{\#}$.* □

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

## 2.2 Sharper Average and Enumerative Estimates

Some of the earlier asymptotic estimates can be refined a little further by methods of an essentially elementary kind. In the first place, Corollary 1.3.3 may be sharpened so as to yield the following analogue of the classical *Dirichlet divisor formula* for $\mathcal{G}$; the stated error estimate is due to S.D. Cohen [4].

(2.2.1) PROPOSITION. *As* $N \to \infty$*,*

$$\overline{d}(N) = Aq^N[AN + 2\gamma_G + A] + O(Nq^{\nu N}),$$

*where* $\gamma_G$ *is the Euler constant of* $\mathcal{G}$.

PROOF. From the equation $d^{\#}(y) = [Z(y)]^2$, it follows (with $R_n = G(n) - Aq^n$ again)

$$\begin{aligned} \overline{d}(N) &= \sum_{n=0}^{N} G(n)G(N-n) = \sum_{n=0}^{N} (Aq^n + R_n)(Aq^{N-n} + R_{N-n}) \\ &= (N+1)A^2q^N + 2Aq^N \sum_{n=0}^{N} R_n q^{-n} + \sum_{n=0}^{N} R_n R_{N-n} \\ &= (N+1)A^2q^N + 2Aq^N \left\{\gamma_G + O(q^{(\nu-1)N})\right\} + \sum_{n=0}^{N} O(q^{\nu n}q^{\nu(N-n)}), \end{aligned}$$

by the proof of Proposition 1.2.2 (ii), and Axiom $\mathcal{A}^{\#}$. This yields the stated formula. □

The next conclusion sharpens Proposition 1.5.4:

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

(2.2.2) PROPOSITION. *As $N \to \infty$,*

$$\begin{aligned}\overline{d_*}(N) &= A[Z(q^{-2})]^{-1}q^N\left[AN + 2\gamma_G + A + \frac{2AZ'(q^{-2})}{q^2Z(q^{-2})}\right] \\ &\quad + \begin{cases} O(N^2q^{\frac{1}{2}N}) & \textit{if } \nu \le \frac{1}{2}, \\ O(Nq^{\nu N}) & \textit{if } \nu > \frac{1}{2}. \end{cases}\end{aligned}$$

PROOF. Since $d_*^{\#}(y) = \mu^{\#}(y^2)d^{\#}(y)$, Proposition 2.2.1 implies :

$$\begin{aligned}\overline{d_*}(N) &= \sum_{2r\le N}\overline{\mu}(r)\overline{d}(N-2r) \\ &= \sum_{r\le\frac{1}{2}N}\overline{\mu}(r)\left\{Aq^{N-2r}[A(N-2r)+2\gamma_G+A]+O(Nq^{\nu(N-2r)})\right\} \\ &= Aq^N[AN+2\gamma_G+A]\sum_{r\le\frac{1}{2}N}\overline{\mu}(r)q^{-2r} - 2A^2q^N\sum_{r\le\frac{1}{2}N}r\overline{\mu}(r)q^{-2r} \\ &\quad + O\left(Nq^{\nu N}\sum_{r\le\frac{1}{2}N}|\overline{\mu}(r)|q^{-2\nu r}\right) \\ &= Aq^N[AN+2\gamma_G+A]\left\{\mu^{\#}(q^{-2})+O\left(\sum_{r>\frac{1}{2}N}q^{-r}\right)\right\} \\ &\quad - 2A^2q^{N-2}\left\{\mu^{\#\prime}(q^{-2})+O\left(\sum_{r>\frac{1}{2}N}rq^{-r}\right)\right\} \\ &\quad + \begin{cases} O(N^2q^{\frac{1}{2}N}) & \text{if } \nu\le\frac{1}{2}, \\ O(Nq^{\nu N}) & \text{if } \nu>\frac{1}{2}. \end{cases}\end{aligned}$$

Now $\sum_{r>\frac{1}{2}N} q^{-r} = O(q^{-\frac{1}{2}N})$, and partial summation (cf. [AB], page 83, say) gives

$$\sum_{r>\frac{1}{2}N} rq^{-r} = -q^{-\frac{1}{2}N}\sum_{r\le\frac{1}{2}N} r + (\log q)\int_{\frac{1}{2}N}^{\infty} q^{-t}\left(\sum_{r\le t} r\right) dt$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

$$\begin{aligned} &= O(N^2 q^{-\frac{1}{2}N}) + O\left(\int_{\frac{1}{2}N}^{\infty} t^2 q^{-t} dt\right) \\ &= O(N^2 q^{-\frac{1}{2}N}), \end{aligned}$$

by partial integration. Substitution in the preceding formula for $\overline{d_*}(N)$ now yields Proposition 2.2.2. □

The following technique for seeking asymptotic estimates, based on relatively elementary complex analysis and ideas of Darboux, is often easier to apply than methods which are "completely elementary". For this reason, the approach is often useful, even though it may not directly yield the sharpest possible estimates in all individual cases.

Suppose that $F(y) = \sum_{n=0}^{\infty} c_n y^n$ is analytic for $|y| \leq R$, with the possible exception of a finite number of poles $z$ for which $|z| < R$, and consider any $r > 0$ such that $F(y)$ is analytic throughout the disc $|y| \leq r$. Then, by Cauchy's integral formula,

$$c_N = \frac{1}{2\pi i} \int_{|y|=r} \frac{F(y)}{y^{N+1}} dy,$$

while, by Cauchy's residue theorem,

$$\left( \int_{|y|=R} - \int_{|y|=r} \right) \frac{F(y)}{y^{N+1}} dy = 2\pi i \sum \operatorname{Res} \frac{F(y)}{y^{N+1}},$$

where the sum extends over the (possibly empty) set of poles of $F(y)$ in $|y| < R$. Hence

$$c_N = -\sum \operatorname{Res} \frac{F(y)}{y^{N+1}} + \frac{1}{2\pi i} \int_{|y|=R} \frac{F(y)}{y^{N+1}} dy.$$

Now, if $h(\theta) = F(Re^{i\theta})$, integration by parts and the fact that $h(\theta)$ is differentiable arbitrarily often show that, for any positive integer $k$,

$$\int_{|y|=R} \frac{F(y)}{y^{N+1}} dy \quad = \quad iR^{-N} \int_0^{2\pi} h(\theta) e^{-Ni\theta} d\theta$$

$$\begin{aligned}
&= -N^{-1}R^{-N}h(\theta)e^{-Ni\theta}\Big|_0^{2\pi} + N^{-1}R^{-N}\int_0^{2\pi} h'(\theta)e^{-Ni\theta}d\theta \\
&= N^{-1}R^{-N}\int_0^{2\pi} h'(\theta)e^{-Ni\theta}d\theta \\
&= \cdots = i^{1-k}N^{-k}R^{-N}\int_0^{2\pi} h^{(k)}(\theta)e^{-Ni\theta}d\theta.
\end{aligned}$$

By the Riemann–Lebesgue lemma of Fourier analysis, the last integral is $o(1)$ as $N \to \infty$. Hence one may deduce:

(2.2.3) LEMMA. *Let $F(y) = \sum_{n=0}^{\infty} c_n y^n$ be analytic for $|y| \leq R$, with the possible exception of a finite number of poles $z$ with $|z| < R$. Then, for any $\alpha \geq 0$,*

$$c_N = -\sum Res \frac{F(y)}{y^{N+1}} + o(N^{-\alpha}R^{-N}) \text{ as } N \to \infty,$$

*where the sum is over the poles of $F(y)$ in $|y| < R$.* □

In many cases, Lemma 2.2.3 reduces the problem of estimating the asymptotic average value of a given arithmetical function $f$ for elements of large degree $N$ to the fairly simple one of calculating the residue of $\frac{f^\#(y)}{y^{N+1}}$ at a suitable point $y$. For example, it leads to the following refinement of Lemma 1.3.2.

(2.2.4) PROPOSITION. *There exists a polynomial $Q_k(N)$ of degree $k-1$ $(k \geq 2)$ in $N$, with leading coefficient $\frac{A^{k-1}}{(k-1)!}$, such that, for any $\alpha > 0$,*

$$\overline{d_k}(N) = Aq^N Q_k(N) + O(N^{-\alpha}q^N) \text{ as } N \to \infty.$$

PROOF. The associated power series of the generalized divisor function $d_k$ satisfies $d_k^\# = [Z(y)]^k$, and so Proposition 1.2.1 implies that $d_k^\#(y)$ is analytic for $|y| < q^{-\nu}$ apart from having a pole at $y = q^{-1}$. Further, Proposition 1.2.1 also implies that, near $y = q^{-1}$, $Z_G(y)$ has an expansion of the form

$$Z_G(y) = \frac{-q^{-1}A}{y - q^{-1}} + g(y),$$

where $g(y)$ is analytic at and near $y = q^{-1}$. Therefore, near $y = q^{-1}$,

$$\begin{aligned}
\frac{d_k^{\#}(y)}{y^{N+1}} &= (q^{-1} + y - q^{-1})^{-N-1}\left[\frac{-q^{-1}A}{y - q^{-1}} + g(y)\right]^k \\
&= q^{N+1}\left\{\sum_{r=0}^{\infty}\binom{-N-1}{r}q^r(y - q^{-1})^r\right\}\left\{\sum_{t=0}^{k}\binom{k}{t}\frac{(-q^{-1}A)^t}{(y - q^{-1})^t}[g(y)]^{k-t}\right\} \\
&= q^{N+1}\left\{\sum_{r=0}^{\infty}\binom{-N-1}{r}q^r(y - q^{-1})^r\right\}\left\{\sum_{t=-k}^{\infty}a_t(y - q^{-1})^t\right\},
\end{aligned}$$

for certain constants $a_t$, with $a_{-k} = (-q^{-1}A)^k$. Hence the residue of $\frac{d_k^{\#}(y)}{y^{n+1}}$ at $y = q^{-1}$ is the quantity

$$q^{N+1}\left[a_{-1} + a_{-2}(-N-1)q + \cdots + a_{-k}\binom{-N-1}{k-1}q^{k-1}\right] = -Aq^N Q_k(N),$$

say, where $Q_k(N)$ is a polynomial of degree $k - 1$ in $N$, whose leading coefficient is

$$-\frac{q}{A}\left\{a_{-k}\frac{(-q)^{k-1}}{(k-1)!}\right\} = \frac{A^{k-1}}{(k-1)!}.$$

In order to deduce the proposition from Lemma 2.2.3 one may now substitute $R = q^{-1} + \varepsilon$ where $\varepsilon > 0$ is a suitable constant. Then Lemma 2.2.3 implies that, for any $\alpha > 0$,

$$\begin{aligned}
\overline{d_k}(N) &= Aq^N Q_k(N) + O\left(N^{-\alpha}(q^{-1} + \varepsilon)^{-N}\right) \\
&= Aq^N Q_k(N) + O(N^{-\alpha}q^N). \qquad \square
\end{aligned}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

It may be noted that Proposition 1.2.2 (ii) implies that the above function $g(y)$ has the value $g(q^{-1}) = \gamma_G$ at $y = q^{-1}$. This leads to the conclusion that the coefficient of $N^{k-2}$ in $Q_k(N)$ is equal to

$$-\frac{q}{A}\left\{a_{-k+1}\frac{(-q)^{k-2}}{(k-2)!} + a_{-k}\frac{(-q)^{k-1}}{(k-1)!}\sum_{r=1}^{k-1}\frac{(k-1)!}{r}\right\}$$

$$= \frac{kA^{k-2}}{(k-2)!}\gamma_G + A^{k-1}\sum_{r=1}^{k-1}\frac{1}{r},$$

since $a_{-k} = (-q^{-1}A)^k$ and $a_{-k+1} = k(-q^{-1}A)^{k-1}\gamma_G$. For $k = 2$, this coefficient therefore reduces to the constant $2\gamma_G + A$ found in Proposition 2.2.1.

By another application of Lemma 2.2.3 one can deduce the following refinement of Proposition 1.5.5:

(2.2.5) PROPOSITION. *There exists a polynomial $Q(N)$ of degree 3 in $N$, with leading coefficient $\frac{1}{6}A^3[Z(q^{-2})]^{-1}$, such that, for any $\alpha > 0$,*

$$\overline{d^2}(N) = Aq^N Q(N) + O(N^{-\alpha}q^N) \text{ as } N \to \infty.$$

PROOF. The details are left as an exercise; the reader may perhaps also care to calculate the coefficients of $Q(N)$. □

It is interesting to compare some of the preceding asymptotic results with the corresponding explicit algebraic one available for the elementary semigroup $\mathcal{G}_q$ of all monic polynomials over $\mathbb{F}_q$. Here the generating function

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

reduces simply to $(1-qy)^{-1}$, and this leads to explicit algebraic formulae for the associated power series of arithmetical functions of the kinds discussed above; compare [AB], Proposition 3.3.2.

For example, in this special case,

$$\begin{aligned} d_k^\#(y) &= (1-qy)^{-k} = \sum_{N=0}^{\infty} \binom{-k}{N} (-q)^N y^N \\ &= \sum_{N=0}^{\infty} \frac{(N+1)(N+2)\ldots(N+k-1)}{(k-1)!} q^N y^N. \end{aligned}$$

Hence $Q_k(N) = \frac{(N+1)(N+2)\ldots(N+k-1)}{(k-1)!}$ for $\mathcal{G}_q$, and here $\overline{d_k}(N) = q^N Q_k(N)$ exactly for all $N \geq 0$.

Also, for the same semigroup,

$$d_*^\#(y) = (1-qy^2)(1-qy)^{-2},\ d^{2\#}(y) = (1-qy^2)(1-qy)^{-4},$$

and so now one obtains the exact equations

$$\overline{d_*}(N) = q^N \left[(1-q^{-1})N + 1 + q^{-1}\right],$$

$$\overline{d^2}(N) = \frac{1}{6} q^N (N+1) \left[(1-q^{-1})N^2 + (5+q^{-1})N + 6\right],$$

for $N \geq 2$.

We conclude this section with an exposition of some refinements of the theorems of Section 2.1, which is based on unpublished joint notes by D.B. Sears and J.N. Ridley [1]. The refinements in question replace the estimates of type $Aq^N + O(q^{\frac{1}{2}N})$ of Theorems 2.1.5 and 2.1.7 by asymptotic series of arbitrary length:

(2.2.6) THEOREM. *For any fixed integer $k \geq 2$, the total number $\mathcal{F}(N)$ of non-isomorphic modules of cardinal $q^N$ in the category $\mathcal{F} = \mathcal{F}_D$ has the*

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

*asymptotic expansion*

$$\mathcal{F}(N) = \sum_{r=1}^{k-1} A_r(N) q^{N/r} + O(q^{N/k}) \text{ as } N \to \infty,$$

*where the* $A_r(N)$ *are numbers (independent of* $k$*) expressible in the form*

$$A_r(N) = \frac{1}{r} A_D \sum_{m=0}^{r-1} e^{-2\pi i mN/r} \prod_{\substack{t=1 \\ t \neq r}}^{\infty} Z_D\left(e^{2\pi i\, mt/r} q^{-t/r}\right).$$

*In addition,*

$$\mathcal{F}(N) = A_D \lim_{k \to \infty} \sum_{r=1}^{k} \frac{1}{r} q^{N/r} \sum_{m=0}^{r-1} e^{-2\pi i mN/r} \prod_{\substack{t=1 \\ t \neq r}}^{k} Z_D\left(e^{2\pi i\, mt/r} q^{-t/r}\right).$$

The proof of this theorem will be combined with that of:

(2.2.7) THEOREM. *For any fixed integer* $k \geq 2$*, the total number* $\mathcal{S}(N)$ *of non–isomorphic algebras of cardinal* $q^N$ *in the category* $\mathcal{S} = \mathcal{S}_D$ *has the asymptotic expansion*

$$\mathcal{S}(N) = \sum_{r=1}^{k-1} B_r(N) q^{N/r} + O(N^{\theta(k)} q^{N/k}) \text{ as } N \to \infty,$$

*for certain numbers* $B_r(N)$ *with* $B_r(N) = O(N^{\delta(r)-1})$ *as* $N \to \infty$*, where* $\theta(k) = \delta(k) - 2 + \max_{1 \leq r < k} \delta(r)$*, and* $\delta(r) = \sum_{d^2 | r} 1$*. In particular, for* $r < 4$*,*

$$B_r(N) = \frac{1}{r} A_D \sum_{m=0}^{r-1} e^{-2\pi i mN/r} \prod_{\substack{s=1 \\ st^2 \neq r}}^{\infty} \prod_{t=1}^{\infty} Z_D\left(e^{2\pi i\, mst^2/r} q^{-st^2/r}\right).$$

PROOFS OF THEOREMS. In view of the identities

$$Z_{\mathcal{F}}(y) = \prod_{r=1}^{\infty} Z_D(y^r), \ Z_{\mathcal{S}}(y) = \prod_{s=1}^{\infty}\prod_{t=1}^{\infty} Z_D(y^{st^2}),$$

which appear (implicitly, in the second case) in the proofs of Theorems 2.1.5 and 2.1.7, the proofs of the present theorems may be combined by initially considering an arbitrary formal power series identity of the form

$$f(y) = \sum_{n=0}^{\infty} a_n y^n = \prod_{r=1}^{\infty} g(y^r)^{\alpha(r)},$$

where $\alpha(r)$ is a positive integer, and $g(y)$ has an expression of the form

$$g(y) = \frac{Q(y)}{1-qy}$$

in which $Q(y)$ denotes an arbitrary polynomial in $y$ with $Q(0) = 1$; here $q$ may be an arbitrary constant greater than 1. In specializing to $Z_{\mathcal{F}}(y)$ and $Z_{\mathcal{S}}(y)$, one is then interested in the two cases:

(i) $\alpha(r) = 1$ for $r \geq 1$, and (ii) $\alpha(r) = \sum_{d^2|r} 1$.

(2.2.8) LEMMA. *For any fixed integer $k \geq 1$, let*

$$f_k(y) = \prod_{r=k}^{\infty} g(y^r)^{\alpha(r)} = \sum_{n=0}^{\infty} b_n y^n,$$

*and suppose that $\alpha(r) = O(r^{\beta})$ as $r \to \infty$, where $\beta$ is constant. Then the series for $f_k(y)$ converges absolutely for $|y| < q^{-1/k}$, and*

$$b_N = O\left(N^{\alpha(k)-1} q^{N/k}\right) \ \textit{as } N \to \infty.$$

*In addition, for $|y| \leq q^{-\varepsilon-1/k} (\varepsilon > 0)$, and any non-negative integer $t$,*

$$\sum_{j>N} j^t b_j y^j = O\left(N^{\alpha(k)+t-1} q^{-\varepsilon N}\right) \ \textit{as } N \to \infty.$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

PROOF. By the assumed form of the function $g(y)$, it follows (as in the discussion of Example 1.1.5) that

$$g(y) = \sum_{n=0}^{\infty} c_n y^n \text{ for } |y| < q^{-1},$$

where $c_n = P(q^{-1})q^n$ for $n \geq \deg P(y)$. Therefore there exists a constant $B > 0$ such that, for $r \geq k \geq 1$ and $|y| \leq \rho < q^{-1/r}$,

$$|g(y^r) - 1| \leq B \sum_{n=1}^{\infty} q^n |y|^{rn} \leq \frac{Bq|y|^r}{1 - q\rho^r} \leq \frac{Bq|y|^r}{1 - q\rho^k}.$$

Hence, for $|y| \leq \rho < q^{-1/k}$,

$$\begin{aligned} \sum_{r=k}^{\infty} \alpha(r)|g(y^r) - 1| &\leq \frac{Bq}{1 - q\rho^k} \sum_{r=k}^{\infty} \alpha(r)|y|^r \\ &\leq \frac{C}{1 - q\rho^k} \sum_{r=k}^{\infty} r^{\beta}\rho^r < \infty, \end{aligned}$$

by the order assumption on $\alpha(r)$, where $C$ is a positive constant. It follows that the power series in $y$ for

$$f_k(y) = \prod_{r=k}^{\infty} \{1 + [g(y^r) - 1]\}^{\alpha(r)}$$

is both uniformly and absolutely convergent for $|y| \leq \rho < q^{-1/k}$; hence $f_k(y)$ is an analytic function of $y$ for $|y| < q^{-1/k}$.

Now note that $f_k(y) = g(y^k)^{\alpha(k)} f_{k+1}(y)$, and that if $g(y^k)^{\alpha(k)} = \sum_{r=0}^{\infty} c'_r y^{rk}$ then each coefficient $c'_r$ occurring here is dominated in absolute value by the coefficient of $y^{rk}$ in the expansion of

$$\left\{B \sum_{n=0}^{\infty} q^n q^{nk}\right\}^{\alpha(k)} = B^{\alpha(k)}(1 - qy^k)^{-\alpha(k)},$$

where $B$ can be chosen to agree with the constant considered earlier. Thus

$$|c'_r| \leq B^M \binom{M+r-1}{M-1} q^r,$$

where $M = \alpha(k)$. Hence, if $f_{k+1}(y) = \sum_{n=0}^{\infty} b'_n y^n$ then

$$\begin{aligned} |b_N| &= \left| \sum_{0 \leq r \leq N/k} c'_r b_{N-rk'} \right| \leq B^M \sum_{r \leq N/k} \binom{M+r-1}{M-1} q^r \, |b_{N-rk'}| \\ &= \frac{B^M}{(M-1)!} q^{N/k} \sum_{r \leq N/k} (r+1)(r+2)\dots(r+M-1) \, |b_{N-rk'}| \, q^{-(N-rk)/k} \\ &= O\left(N^{M-1} q^{N/k}\right) \text{ as } N \to \infty, \end{aligned}$$

since the power series in $y$ for $f_{k+1}(y)$ is absolutely convergent for $|y| < q^{-1/(k+1)}$.

Lastly, for $|y| \leq q^{-\varepsilon - 1/k} (\varepsilon > 0)$, and any non-negative integer $t$,

$$\sum_{j>N} j^t b_j y^j = O\left( \sum_{j>N} j^{t+M-1} q^{j/k} q^{j(-\varepsilon-1/k)} \right) = O\left( \sum_{j>N} j^{t+M-1} q^{-\varepsilon j} \right).$$

Now, for any non-negative integer $m$, and $0 < x < 1$, consider

$$\begin{aligned} \sum_{j>N} j^m x^j &= \sum_{r=0}^{\infty} (N+r+1)^m x^{N+r+1} \\ &= \sum_{r=0}^{\infty} \left\{ \sum_{s=0}^{m} \binom{m}{s} (N+1)^{m-s} r^s \right\} x^{N+r+1} \\ &= x^{N+1} \sum_{s=0}^{m} \binom{m}{s} (N+1)^{m-s} \sum_{r=0}^{\infty} r^s x^r = O(N^m x^N) \end{aligned}$$

as $N \to \infty$. This conclusion then yields the final assertion of the lemma. □

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Continuing our discussion of the initial function $f(y)$, now write it as $F(y) = F_k(y)f_k(y)$ $[k \geq 2]$, where $F_k(y) = \prod_{r=1}^{k-1} g(y^r)^{\alpha(r)}$, and $f_k(y)$ is defined as in Lemma 2.2.8. Then $F_k(y)$ is a rational function of $y$, and so it has a partial fraction decomposition which may be written in the form

$$F_k(y) + S(y) + \sum_{r=1}^{k-1} \sum_{m=0}^{r-1} \sum_{t=1}^{\alpha(r)} \mathbf{c}(r,m,t) \left(1 - q^{1/r} e^{-2\pi i\, m/r} y\right)^{-t},$$

where $S(y)$ is a polynomial in $y$, and the $\mathbf{c}(r,m,t)$ are constants. In particular, for later purposes we note that, if $\alpha(r) = 1$ then one may use l'Hospital's limit rule to deduce that the ensuing constant

$$\begin{aligned} \mathbf{c}(r,m,1) &= \lim_{y \to q^{-1/r} e^{2\pi i\, m/r}} \left(1 - q^{1/r} e^{-2\pi i\, m/r} y\right) F_k(y) \\ &= \frac{1}{r} Q(q^{-1}) \prod_{\substack{t=1 \\ t \neq r}}^{k-1} g\left(e^{2\pi i\, mt/r} q^{-t/r}\right)^{\alpha(t)}. \end{aligned}$$

In general, the partial fraction decomposition of $F_k(y)$ leads to a power series expansion $F_k(y) = \sum_{n=0}^{\infty} \gamma_n y^n$ for $|y| < q^{-1}$, so that (if $S(y) = \sum_{n=0}^{\infty} \delta_n y^n$)

$$F_k(y) - S(y) = \sum_{n=0}^{\infty} \varepsilon_n y^n \text{ for } |y| < q^{-1},$$

with $\varepsilon_n = \gamma_n - \delta_n$. (Since $S(y)$ is a polynomial, of degree $T$ say, it follows that $\delta_n = 0$ and $\varepsilon_n = \gamma_n$ for $n > T$. Here $\gamma_n$ *should not* be confused with the earlier generalized Euler constants.)

Now, as in Lemma 2.2.8 assume that $\alpha(r) = O(r^{\beta})$ as $r \to \infty$, where $\beta$ is constant. Then the coefficient $a_N$ of $y^N$ in the Taylor expansion of $f(y)$ about the origin is given (for $N \geq T$) by

$$\begin{aligned} a_N &= \sum_{j=0}^{N} b_j \gamma_{N-j} = b_N \delta_0 + \cdots + b_{N-T}\delta_T + \sum_{j=0}^{N} b_j \varepsilon_{N-j} \\ &= O\left(N^{\alpha(k)-1} q^{N/k}\right) + \sum_{j=0}^{N} b_j \varepsilon_{N-j} \text{ as } N \to \infty, \end{aligned}$$

by Lemma 2.2.8. Further,

$$\sum_{j=0}^{N} b_j \varepsilon_{N-j} = \sum_{r=1}^{k-1} q^{N/r} \sum_{m=0}^{r-1} e^{-2\pi i m N/r} \sum_{t=1}^{\alpha(r)} c(r,m,t)\Sigma^{(N)},$$

where

$$\Sigma^{(N)} = \sum_{j=0}^{N} \binom{N-j+t-1}{t-1} b_j \left(e^{2\pi i m/r} q^{-1/r}\right)^j .$$

Since the binomial coefficient $\binom{N-j+t-1}{t-1}$ can be written as a polynomial $\xi_0(N) + \xi_1(N)j + \cdots + \xi_{t-1}(N)j^{t-1}$ in which each coefficient $\xi_s(N)$ is itself a polynomial in $N$ (depending on $t$ and of degree at most $t-1$), the last sum $\Sigma^{(N)}$ can be written in the form

$$\begin{aligned}\Sigma^{(N)} &= \sum_{s=0}^{t-1} \xi_s(N) \sum_{j=0}^{N} j^s b_j \left(e^{2\pi i m/r} q^{-1/r}\right)^j \\ &= \sum_{s=0}^{t-1} \xi_s(N) \left\{ \eta_s - \sum_{j>N} j^s b_j \left(e^{2\pi i m/r} q^{-1/r}\right)^j \right\},\end{aligned}$$

where

$$\eta_s = \sum_{j=0}^{\infty} j^s b_j \left(e^{2\pi i m/r} q^{-1/r}\right)^j ;$$

this last series converges since $f_k(y)$ is analytic in $y$ for $|y| < q^{-1/k}$. Therefore

$$\Sigma^{(N)} = \sum_{s=0}^{t-1} \eta_s \xi_s(N) + O\left(N^{t+\alpha(k)-2} q^{\left(\frac{1}{k}-\frac{1}{r}\right)N}\right) \text{ as } N \to \infty,$$

since Lemma 2.2.8 implies that

$$\sum_{j>N} j^s b_j \left(e^{2\pi i m/r} q^{-1/r}\right)^j = O\left(N^{s+\alpha(k)-1} q^{\left(\frac{1}{k}-\frac{1}{r}\right)N}\right).$$

This conclusion about $\Sigma^{(N)}$ then implies that, as $N \to \infty$,

$$\sum_{j=0}^{N} b_j \varepsilon_{N-j} = \sum_{r=1}^{k-1} \left\{ C_r(N) q^{N/r} + O\left(N^{\alpha(r)+\alpha(k)-2} q^{N/k}\right) \right\}$$

$$= \sum_{r=1}^{k-1} C_r(N) q^{N/r} + O\left(N^{\theta(k)} q^{N/k}\right),$$

where $\theta(k) = \alpha(k) - 2 + \max\{\alpha(1), \ldots, \alpha(k-1)\}$. Thus, for any fixed integer $k \geq 2$, the coefficient $a_N$ of $y^N$ in the Taylor expansion of $f(y)$ about the origin can be expressed in the form

$$a_N = \sum_{r=1}^{k-1} C_r(N) q^{N/r} + O\left(N^{\theta(k)} q^{N/k}\right) \text{ as } N \to \infty.$$

In order to complete the present proof, it remains to make some comments about the coefficients $C_r(N)$ appearing in the last asymptotic formula. Firstly, in order to see that the formula does give successively better approximations to $a_N$, we note that the above argument implies that

$$C_r(N) = O\left(N^{\alpha(r)-1}\right) \text{ as } N \to \infty.$$

Secondly, it may be observed that, if $\alpha(r) = 1$ for $r < k$, then the earlier multiple-sum expression for $\sum_{j=0}^{N} b_j \varepsilon_{N-j}$ together with the subsequent discussion of the term $\Sigma^{(N)}$ leads to the formula:

$$\begin{aligned}\sum_{j=0}^{N} b_j \varepsilon_{N-j} &= \sum_{r=1}^{k-1} q^{N/r} \sum_{m=0}^{r-1} e^{-2\pi i mN/r} \boldsymbol{c}(r, m, 1) \Big\{ f_k(e^{2\pi i m/r} q^{-1/r}) \\ &\qquad + O\left(N^{\alpha(k)-1} q^{\left(\frac{1}{k} - \frac{1}{r}\right)N}\right) \Big\}.\end{aligned}$$

Hence the earlier evaluation of $\boldsymbol{c}(r, m, 1)$ in the case when $\alpha(r) = 1$ implies that, if $\alpha(r) = 1$ for $r < k$, then $\theta(k) = \alpha(k) - 1$, and

$$C_r(N) = \frac{1}{r} P(q^{-1}) \sum_{m=0}^{r-1} e^{-2\pi i mN/r} \prod_{\substack{t=1 \\ t \neq r}}^{\infty} g\left(e^{2\pi i mt/r} q^{-t/r}\right)^{\alpha(t)}.$$

This last equation shows that $C_r(N)$ is independent of $k$ and that $C_1(N)$ is also independent of $N$. It also now yields the expression for $A_r(N)$ in

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Theorem 2.2.6 since, in the context of that theorem, $\alpha(r) = 1$ for all $r$. Similarly it yields the evaluation of $B_r(N)$ $[r < 4]$ stated in Theorem 2.2.7.

Lastly we observe that the final assertion of Theorem 2.2.6 is a consequence of the earlier evaluation of $\mathbf{c}(r, m, 1)$ when $\alpha(r) = 1$, together with the fact that $F_k(y) \to f(y)$ uniformly as $k \to \infty$ (for $|y| \leq \rho$ and arbitrary $\rho < q^{-1}$). $\square$

In the special case in which $D$ is the Galois polynomial ring $\mathbb{F}_q[X]$, it follows from Theorem 2.1.1 that the coefficient $A_1 = A_1(N)$ in the asymptotic formula of Theorem 2.2.6 reduces to $P_0(q^{-1})$, where $P_0(y)$ is the classical *partition* generating function. It has been shown by J.N. Ridley and D.B. Sears [1] that, *in this special case, all the coefficients* $A_r(N)$ can be expressed in terms of values of certain *extended* partition generating functions; $\mathcal{F}_q(N)$ also satisfies the simple algebraic formula:

$$F_q(N) = \sum_{r=0}^{N} \rho_r(N - r) q^r,$$

where $\rho_r(n)$ denotes the total number of partitions of $n$ into parts of size at most $r$. *In addition*, still for $D = \mathbb{F}_q[X]$, these authors (*loc. cit.*) have proved a remarkable theorem to the effect that: *The asymptotic series of Theorem 2.2.6 provides a* **convergent** *infinite series representation*

$$F_q(N) = \sum_{r=1}^{\infty} A_r(N) q^{N/r} \textit{ for all } N \geq 0$$

**if and only if** $q \geq 13$.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

# CHAPTER 3

# ABSTRACT PRIME NUMBER THEOREMS (I)

## 3.1 General Remarks and Preliminary Results

In the contexts to be considered in the next sections and later, which involve hypotheses like Axiom $\mathcal{A}^{\#}$ or weaker forms of this axiom, we shall show that there exist both abstract prime number theorems which are closely analogous to the classical Prime Number Theorem for $\mathbb{N}$, and also theorems which diverge significantly from the classical type of conclusion. The latter results will be discussed more fully in Chapter 5.

The abstract prime number theorem of "classical–type" may be viewed as generalizations of the concrete asymptotic enumeration theorems (0.2) and (3.1.1 – 6) in sub–section 3.1.1 below. The latter enumeration results stem from the main concrete examples of natural additive arithmetical semigroups satisfying Axiom $\mathcal{A}^{\#}$, which were introduced in Section 1.1 earlier. They centre strongly around hypotheses entailing Axiom $\mathcal{A}^{\#}$, and the existence of suitably large zero free regions for the generating function $Z(y)$.

In this connection, a somewhat unexpected and paradoxical situation arose in the development of this topic. Axiom $\mathcal{A}^{\#}$ appears initially to provide a comprehensive simple way of encoding the general counting behaviour of the concrete motivating examples of Section 1.1. In the first two chap-

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

ters, it provided a convenient basis for uniformly deriving information on the asymptotic behaviour of arithmetical functions and densities within the context of the main examples, together with the possibility of potential new applications to any further concrete examples of interest which might arise in future. In this way, Axiom $\mathcal{A}^{\#}$ appeared to provide a kind of direct "polynomial type" or "function–field type" of parallel to the rôle of the Axiom $\mathcal{A}$ treated in [AB], which generalizes the asymptotic behaviour of classical and algebraic number theory, together with that of algebraic examples parallel in nature to those of Section 1.1.

Regarding the counting of "primes" Axiom $\mathcal{A}$ leads to uniform generalizations of the classical Prime Number Theorem for $\mathbb{N}$, and parallel theorems within algebraic number theory. Consequently one might have expressed Axiom $\mathcal{A}^{\#}$ to directly lead to similar uniform generalizations of the "classical–type" asymptotic enumeration conclusions (0.2) and (3.1.1 to 6) in sub–section 3.1.1 below, particularly since the Axiom $\mathcal{A}^{\#}$ type of situation appears at first sight to be somewhat "simpler" than that which surrounds Axiom $\mathcal{A}$. Paradoxically, despite some positive initial contributions towards these questions (cf. say J. Knopfmacher [3], [ANAL], Section 8, and S.D. Cohen [1]), it turned out that Axiom $\mathcal{A}^{\#}$ by itself does not suffice for this in all cases. Indlekofer, Manstavicius, Warlimont and W.–B. Zhang showed that a single unexpected and awkward zero of the generating function can possibly occur if only Axiom $\mathcal{A}^{\#}$ is assumed, and this leads to the non–classical type of theorems referred to above.

Such an extra zero *does not* occur for the original motivating examples which led to Axiom $\mathcal{A}^{\#}$ on the grounds of naturally–occurring, pre–existing situations in other parts of mathematics (cf. Section 1.1). Nevertheless, theoretical analytical examples can be constructed (cf. say Indlekofer, Manstavicius and Warlimont [1], Zhang [1], and Example 3.8.1 below) for which there is such a zero, although *no examples* have been exhibited up to now *in which* such a zero occurs in any pre–existing, naturally interesting, context. If one bears in mind the emphasis in Chapters 1 and 2 on concrete, natural applications of the general discussion, this leads to a divergence in approaches to further investigations:

On the one hand, the simple and seemingly appropriate choice of Axiom $\mathcal{A}^\#$ as a basic assumption might be regarded as an incomplete encoding of the fundamental situation to be unified by appropriate axiomatic hypotheses, and some additional hypothesis or axiom could be introduced so as to *both include* all the desired applications, *and exclude* the "pathological" extra zero which leads to the theoretical non–classical abstract prime number theorems (which have *not yet* admitted any significant natural applications).

On the other hand, one could continue to study *all possible* consequences of both Axiom $\mathcal{A}^\#$ and some weaker forms of this axiom, *purely for* the theoretical interest of the implications derived, and *without* special emphasis on other mathematical applications.

Although the main emphasis and spirit of the first author's earlier monographs [AB] and [ANAL] is more in keeping with the first alternative above, the present monograph will also admit *some compromises* by including certain results and discussions of them in the spirit of the second alternative. At the same time, various other results will restrict attention to the "classical" type of situation, in view of the more concrete applicability of this case.

### 3.1.1 Prime counting estimates in concrete cases

Within the context of the main natural examples given in Section 1.1 for the concrete occurrence of cases of Axiom $\mathcal{A}^\#$, it is actually possible to obtain both exact and asymptotic formulae for the relevant numbers $P(m)$:

Firstly consider the elementary semigroup $\mathcal{G}_q$ of all monic polynomials in a Galois polynomial ring $\mathbb{F}_q[X]$. A well known theorem about polynomials over finite fields (cf. say Chapter 3 of Lidl and Niderreiter [1], or [AB], Proposition 3.2.3), states that the total number $P_q(m)$ of *irreducible* polynomials of degree $m$ in $\mathcal{G}_q$ satisfies the exact equation

$$P_q(m) = \frac{1}{m}\sum_{d|m}\mu(d)q^{m/d}, \tag{0.1}$$

where $\mu$ denotes the classical Möbius function on the positive integers. Therefore

$$\begin{aligned} P_q(m) &= \frac{1}{m}\left\{q^m + \sum_{2\leq d|m}\mu(d)q^{m/d}\right\} \\ &= \frac{1}{m}\left\{q^m + O\left(q^{\frac{1}{2}m}\right) + O\left(\sum_{3\leq d|m} q^{m/d}\right)\right\} \\ &= \frac{1}{m}\left\{q^m + O\left(q^{\frac{1}{2}m}\right) + O\left(mq^{\frac{1}{3}m}\right)\right\} \\ &= \frac{q^m}{m} + O\left(\frac{q^{\frac{1}{2}m}}{m}\right). \end{aligned} \tag{0.2}$$

This last conclusion may be regarded as the asymptotic "prime number theorem" for the special semigroup $\mathcal{G}_q$.

Now let $P_{\mathcal{F}}(m)$ denote the total number of non–isomorphic *indecomposable modules* of cardinal $q^m$ in the category $\mathcal{F} = \mathcal{F}_q$ described in Example 1.1.2 of Section 1.1.

(3.1.1) PROPOSITION. *The total number $P_{\mathcal{F}}(m)$ of non–isomorphic indecomposable modules of cardinal $q^m$ satisfies:*

$$P_{\mathcal{F}}(m) \;=\; \sum_{r|m}P_q(r) = \sum_{r|m}\frac{1}{r}\sum_{d|r}\mu(d)q^{r/d}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

$$= \frac{q^m}{m} + O\left(\frac{q^{\frac{1}{2}m}}{m}\right) \quad \textit{as } m \to \infty.$$

PROOF. By the discussion of $\mathcal{F}$ in Example 1.1.2, every indecomposable finite module over $\mathbb{F}_q[X]$ is isomorphic to a module of the form $\mathbb{F}_q[X]/(p^r)$, where $p$ is an irreducible polynomial and $r$ is a positive integer, and conversely all such modules are indecomposable. Further, the cardinality of this module is $q^{r \deg p}$. Therefore

$$\begin{aligned} P_{\mathcal{F}}(m) &= \sum_{r \deg p = m} 1 = \sum_{r|m} \sum_{\deg p = \frac{m}{r}} 1 \\ &= \sum_{r|m} P_q\left(\frac{m}{r}\right) = \sum_{r|m} P_q(r). \end{aligned}$$

The explicit formula for $P_q(m)$ quoted above then leads to the stated explicit formula for $P_{\mathcal{F}}(m)$, while the above asymptotic formula for $P_q(m)$ now implies that

$$\begin{aligned} P_{\mathcal{F}}(m) &= P_q(m) + \sum_{2 \le r|m} P_q\left(\frac{m}{r}\right) \\ &= P_q(m) + O\left(\sum_{3 \le r|m} \frac{q^{m/r}}{m/r}\right) + O\left(\frac{q^{\frac{1}{2}m}}{\frac{1}{2}m}\right) \\ &= \frac{q^m}{m} + O\left(\frac{q^{\frac{1}{2}m}}{m}\right) + O\left(mq^{\frac{1}{3}m}\right), \end{aligned}$$

as $m \to \infty$. □

Another specific example of an additive arithmetical semigroup for which it is easy to give a direct proof of an asymptotic "prime number theorem" is given by the semigroup associated with the category $\mathcal{S} = \mathcal{S}_q$ described in Example 1.1.3 of Section 1.1:

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

(3.1.2) PROPOSITION. *The total number $P_{\mathcal{S}}(m)$ of non-isomorphic simple algebras of cardinal $q^m$ in $\mathcal{S}$ satifies:*

$$\begin{aligned} P_{\mathcal{S}}(m) &= \sum_{k^2|m} P_{\mathcal{F}}\left(\frac{m}{k^2}\right) = \sum_{k^2|m} \sum_{r|\frac{m}{k^2}} \frac{1}{r} \sum_{d|r} \mu(d) q^{r/d} \\ &= \frac{q^m}{m} + O\left(\frac{q^{\frac{1}{2}m}}{m}\right) \quad \textit{as } m \to \infty. \end{aligned}$$

PROOF. According to Example 1.1.3, the *simple* finite algebras over $\mathbb{F}_q[X]$ are isomorphic to the various total matrix algebras of the form $M_k(F_r)$ $[k, r = 1, 2, \ldots]$, where $F_r$ is a field extension of degree $r$ of the field $F_1 = F_q[X]/(p)$ ($p$ a prime polynomial); further, $M_k(F_r)$ has cardinal $q^{rk^2 \deg p}$. Hence

$$\begin{aligned} P_{\mathcal{S}}(m) &= \sum_{rk^2 \deg p = m} 1 = \sum_{k^2|m} \sum_{r \deg p = \frac{m}{k^2}} 1 \\ &= \sum_{k^2|m} P_{\mathcal{F}}\left(\frac{m}{k^2}\right), \end{aligned}$$

by the first equation for $P_{\mathcal{F}}(m)$ in the proof of Proposition 3.1.1. The asymptotic formula for $P_{\mathcal{S}}(m)$ may then be deduced from that for $P_{\mathcal{F}}(m)$ by a slight variation of the preceding proof of the asymptotic formula for that function. □

Similar sharp conclusions may be derived for the other concrete examples of arithmetical semigroups satisfying Axiom $\mathcal{A}^{\#}$ that were discussed in Section 1.1. These examples all arise from consideration of an algebraic function field $K$ in one variable over the finite field $\mathbb{F}_q$, and the principal order $D$ in $K$, and also the categories $\mathcal{F}_D$, $\mathcal{S}_D$ generalizing $\mathcal{F}_q$ and $\mathcal{S}_q$. As before, our starting point for dealing with these examples will be the

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

equation for the zeta function of $K$ quoted under Example 1.1.4:

$$\zeta_K(z) = \frac{L(q^{-z})}{(1-q^{-z})(1-q^{1-z})},$$

where $L(q^{-z})$ is a polynomial with rational integer coefficients in $q^{-z}$. In the treatment of Example 1.1.5, it was noted that $K$ has only a finite number of prime divisors that cannot be identified with prime ideals in the ring $D$, so that by multiplying by the product over those former prime divisors $\mathbf{p}$ one obtains the zeta function

$$\zeta_D(z) = \zeta_K(z) \prod_{\mathbf{p}} \left(1 - N(\mathbf{p})^{-z}\right) = \frac{Q(q^{-z})}{1-q^{1-z}},$$

where $Q(q^{-z})$ is also a polynomial with integer coefficients in $q^{-z}$. By the theorem of Weil quoted in Section 1.1, which implies that every zero $z$ of $L(q^{-z})$ has real part $\frac{1}{2}$, and by Lemma 3.1.4 below, we now obtain:

(3.1.3) THEOREM. *Let $P_K(m)$ denote the total number of prime divisors of degree $m$ in $K$, and let $P_D(m)$ denote the total number of prime ideals of degree $m$ in $D$. Then, as $m \to \infty$,*

$$P_K(m) = \frac{q^m}{m} + O\left(\frac{q^{\frac{1}{2}m}}{m}\right) = P_D(m). \qquad \square$$

(3.1.4) LEMMA. *Let $\mathcal{G}$ denote any additive arithmetical semigroup whose generating function can be expressed in the form*

$$Z(y) = \frac{Q(y)}{1-qy},$$

*where $Q(y) = \prod_{i=1}^{M}(q - \alpha_i y)$, $\alpha_i$ complex, is a polynomial in $y$. Then the total number $P(m)$ of primes of degree $m$ in $\mathcal{G}$ is given by*

$$P(m) = \frac{1}{m} \sum_{d|m} \mu\left(\frac{d}{m}\right) \left[q^d - \alpha_1^d - \cdots - \alpha_M^d\right],$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

*where $\mu$ is the classical Möbius function. Hence, as $m \to \infty$,*

$$P(m) = \frac{q^m}{m} + O\left(\frac{q^{\theta m}}{m}\right),$$

*where* $q^\theta = \max\left\{q^{\frac{1}{2}}, |\alpha_1|, \ldots, |\alpha_M|\right\}$.

Proof. The case of the special semigroup $\mathcal{G}_q$ is covered by this lemma if we take $Q(y) = 1$. The present proof extends that of Proposition 3.2.3 of [AB], which deals with $\mathcal{G}_q$ directly:

Firstly, consider the logarithmic derivative $\mathrm{D_L}(f) = f'/f$ of an invertible formal power series $f$. As in [AB], page 61, the Euler product formula

$$Z(y) = \prod_{m=1}^{\infty} (1 - y^m)^{-P(m)}$$

leads to the formula

$$\mathrm{D_L}(Z(y)) = \sum_{m=1}^{\infty} mP(m)y^{m-1}\left\{1 + y^m + y^{2m} + \cdots\right\}.$$

At the same time,

$$\begin{aligned}\mathrm{D_L}(Z(y)) &= \mathrm{D_L}(Q(y)) + \mathrm{D_L}((1-qy)^{-1}) \\ &= -\sum_{i=1}^{M} \frac{\alpha_i}{1-\alpha_i y} + \sum_{n=0}^{\infty} q^{n+1}y^n \\ &= \sum_{n=0}^{\infty}\left(q^{n+1} - \sum_{i=1}^{M}\alpha_i^{n+1}\right)y^n.\end{aligned}$$

Comparison of the coefficients in the two expressions then yields the equations

$$q^m - \alpha_1^m - \cdots - \alpha_M^m = \sum_{\substack{k\geq 1, r\geq 0\\ k-1+rk=m-1}} kP(k) = \sum_{d|m} dP(d).$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

The stated algebraic equation for $P(m)$ therefore follows by ordinary Möbius inversion.

For the required asymptotic formula, one may now deduce that

$$\begin{aligned} P(m) &= \frac{1}{m}\left\{q^m - \alpha_1^m - \cdots - \alpha_M^m + \sum_{d|m,\frac{m}{d}\geq 2} \mu\left(\frac{m}{d}\right)\left[q^d + O(q^{\theta d})\right]\right\} \\ &= \frac{1}{m}\left\{q^m + O(q^{\theta m}) + O\left(q^{\frac{1}{2}m}\right) + O\left(\sum_{d\leq\frac{1}{3}m}\left[q^d + O(q^{\theta d})\right]\right)\right\} \\ &= \frac{1}{m}\left\{q^m + O(q^{\theta m})\right\}. \qquad \square \end{aligned}$$

Now consider the categories $\mathcal{F} = \mathcal{F}_D$ and $\mathcal{S} = \mathcal{S}_D$ defined in Examples 1.1.6 and 1.1.7, relative to the principal order $D$ in the algebraic function field $K$ discussed earlier.

(3.1.5) THEOREM. *Let $P_{\mathcal{F}}(m)$ denote the total number of non-isomorphic indecomposable modules of cardinal $q^m$ in $\mathcal{F}$. Then*

$$\begin{aligned} P_{\mathcal{F}}(m) &= \sum_{r|m} P_D(r) \\ &= \frac{q^m}{m} + O\left(\frac{q^{\frac{1}{2}m}}{m}\right) \quad \textit{as } m \to \infty. \end{aligned}$$

PROOF. This theorem follows in essentially the same way as Proposition 3.1.1 earlier, after it has been observed that the description of the indecomposable modules in $\mathcal{F}$ given under Example 1.1.6 implies that

$$P_{\mathcal{F}}(m) = \sum_{\mathrm{N}(\mathbf{p})^r = q^m} 1 = \sum_{r|m} \sum_{\mathrm{N}(\mathbf{p}) = q^{m/r}} 1$$

$$= \sum_{r|m} P_D\left(\frac{m}{r}\right) .$$

The asymptotic formula then follows with the aid of Theorem 3.1.3. □

In a similar way, one may now deduce:

(3.1.6) THEOREM. *Let $P_{\mathcal{S}}(m)$ denote the total number of non-isomorphic simple algebras of cardinal $q^m$ in $\mathcal{S}$. Then*

$$\begin{aligned} P_{\mathcal{S}}(m) &= \sum_{k^2|m} P_{\mathcal{F}}\left(\frac{m}{k^2}\right) \\ &= \frac{q^m}{m} + O\left(\frac{q^{\frac{1}{2}m}}{m}\right) \quad \textit{as } m \to \infty. \end{aligned} \qquad \square$$

Lastly, we note that Example 1.1.8 also involves exact and sharp asymptotic conclusions, via the earlier equations (0.1) and (0.2) for $P_q(m)$, and the next proposition.

(3.1.6) PROPOSITION. *The total number $P_{q,2}(m)$ of primes of degree $m$ in the semigroup $\mathcal{H}_{q,2}$ of Example 1.1.8 satisfies*

$$P_{q,2}(m) = \begin{cases} q+1 & \textit{if } m = 1, \\ P_q(m) & \textit{if } m > 1. \end{cases}$$

PROOF. The equation for $H_{q,k}(n)$ under Example 1.1.8 shows that

$$H_{q,2}(n) = \frac{q^{n+1}-1}{q-1},$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

and so the generating function for $\mathcal{H}_{q,2}$ is

$$\begin{aligned} Z(y) &= \sum_{n=0}^{\infty}\left(\sum_{0\le r\le n} q^r\right) y^n = \sum_{r=0}^{\infty} q^r \sum_{n=r}^{\infty} y^n \\ &= \sum_{r=0}^{\infty}\frac{q^r y^r}{1-y} = \frac{1}{(1-y)(1-qy)}. \end{aligned}$$

Thus the Euler product formula for $\mathcal{G}_q$ yields

$$Z(y) = \frac{1}{1-y}\prod_{m=1}^{\infty}(1-y^m)^{-P_q(m)}.$$

Hence (3.1.6) follows. □

## 3.1.2 Additive convolution of ordinary arithmetical functions

In the further discussion, we shall apply some techniques of additive convolution of ordinary arithmetical functions of non–negative integers. In this subsection we introduce the elementary theory of *additive* convolution first.

A complex–valued function $f(n)$ defined for all non–negative integers $n$ will here be called an (**ordinary**) **arithmetical** function. The addition of arithmetical functions $f$ and $g$, and scalar multiplication by $\lambda \in \mathbb{C}$, are defined by setting

$$(f+g)(n) = f(n) + g(n), \quad (\lambda f)(n) = \lambda f(n).$$

The function $h$ defined by setting

$$h(n) = \sum_{k=0}^{n} f(k)g(n-k), \quad \text{for } n = 0, 1, 2, \ldots,$$

is called the **additive** (or **Cauchy**) **convolution** of $f$ and $g$, and denoted by $f * g$. It is easy to see that additive convolution is commutative and associative. Also, the additive convolution and addition are distributive in the sense that

$$f * (g + h) = f * g + f * h.$$

Moreover, for $\lambda \in \mathbb{C}$,

$$\lambda(f * g) = (\lambda f) * g = f * (\lambda g).$$

The function

$$e(n) = \begin{cases} 1, & \text{for } n = 0, \\ 0, & \text{for } n \geq 1, \end{cases}$$

is the additive–convolution *identity*, that is

$$f * e = e * f = f$$

for every arithmetical function $f$. Therefore, arithmetical functions under addition, scalar multiplication, and additive convolution form a commutative algebra with identity. In this algebra, we have the following useful inequality

$$|f * g| \leq |f| * |g|, \tag{1.1}$$

which is easily verified.

If there exists an arithmetical function $f^{-1}$ such that $f * f^{-1} = f^{-1} * f = e$ then $f$ is said to be invertible and $f^{-1}$ is called an (additive–convolution) *inverse* of $f$. The equation $f * f^{-1} = e$ is equivalent to the infinite system of equations

$$\begin{aligned} 1 &= f(0)f^{-1}(0), \\ 0 &= f(0)f^{-1}(1) + f(1)f^{-1}(0), \\ 0 &= f(0)f^{-1}(2) + f(1)f^{-1}(1) + f(2)f^{-1}(0), \\ &\vdots \end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Hence it is clear that $f(0) \neq 0$ is necessary for the existence of an inverse $f^{-1}$. This condition is also sufficient. Actually, if $f(0) \neq 0$ the first equation of the above system gives the value $f^{-1}(0)$. Then, by induction, knowing $f^{-1}(0), f^{-1}(1), \ldots, f^{-1}(n-1)$ from the first $n$ equations of the system, the value $f^{-1}(n)$ is given, from the $(n+1)$-th equation, by

$$f^{-1}(n) = -\frac{1}{f(0)} \sum_{k=1}^{n} f(k) f^{-1}(n-k).$$

Therefore, *an arithmetical function $f$ is invertible if and only if $f(0) \neq 0$.*

We define a *differentiation* operator $L$ on the algebra of arithmetical functions $f$ by setting

$$(Lf)(n) = nf(n), \quad n = 0, 1, 2, \ldots . \tag{1.2}$$

The operator L is an analogue of the "differentiation" operator defined on the algebra of arithmetical functions of a *positive* integer, under addition, scalar multiplication, and *multiplicative* (or *Dirichlet*) convolution (see e.g. Apostol [1], Chapter 2). It has the important derivative property

$$L(f * g) = Lf * g + f * Lg. \tag{1.3}$$

This is easily verified from the equation

$$n \sum_{k=0}^{n} f(k) g(n-k) = \sum_{k=0}^{n} k f(k) g(n-k) + \sum_{k=0}^{n} f(k)(n-k) g(n-k).$$

We define $L^k f = L(L^{k-1} f)$, $k = 2, 3, \ldots$, recursively. Then the general *Leibniz formula*

$$L^m(f * g) = \sum_{\ell=0}^{m} \binom{m}{\ell} (L^{m-\ell} f) * (L^{\ell} g) \tag{1.4}$$

is easily verified by induction. In particular, we have

$$L^2(f * g) = L^2 f * g + 2Lf * Lg + f * L^2 g. \tag{1.5}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

**Note:** In certain situations it may be useful to consider *both* the above additive convolution $*_0 = *$ *and* the *Dirichlet–type* convolution $*_1$ only (denoted by $*$ in [AB], Chapter 2). In such cases, the notations $*_0$ and $*_1$ will be introduced in order to avoid confusion.

### 3.1.3 Generating functions and von Mangoldt's function

Let $f$ be an ordinary arithmetical function (defined for all non–negative integers $n$). In line with common usage, the *generating function* of $f$ is, by definition,

$$\hat{f}(y) = \sum_{n=0}^{\infty} f(n) y^n.$$

Here the right–hand side is a convergent power series under certain conditions on the growth of magnitude of $|f(n)|$; note that $f(0) = \hat{f}(0)$. *Hence $f$ is invertible if and only if $\hat{f}(0) \neq 0$.* We also note that the generating function of $Lf$ is

$$\sum_{n=0}^{\infty} n f(n) y^n = y \hat{f}'(y).$$

If $h = f * g$ is the (additive) convolution of functions $f$ and $g$, then the generating function $\hat{h}(y)$ of $h$ satisfies

$$\hat{h}(y) = \hat{f}(y)\hat{g}(y).$$

We note that the generating function of $Lh$ is

$$\begin{aligned}(Lh)\hat{}\,(y) = y\hat{h}'(y) &= (y\hat{f}'(y))\hat{g}(y) + \hat{f}(y)(y\hat{g}'(y)) \\ &= (Lf)\hat{}\,(y)\hat{g}(y) + \hat{f}(y)(Lg)\hat{}\,(y),\end{aligned}$$

which is the generating function form of (1.3) above.

Let now $(\mathcal{G}, \partial)$ be an additive arithmetical semigroup, with Euler product formula

$$Z(y) = \sum_{n=0}^{\infty} G(n) y^n = \prod_{m=1}^{\infty} (1 - y^m)^{-P(m)}. \tag{1.6}$$

In the further discussion, information about $P(m)$ will be derived from this formula with the aid of the von Mangoldt function $\Lambda$ defined on $\mathcal{G}$ by setting

$$\Lambda(a) = \begin{cases} \partial(p), & \text{if } a \text{ is a prime power } p^r \neq 1; \\ 0, & \text{otherwise,} \end{cases}$$

which is an analogue for $\mathcal{G}$ of the classical von Mangoldt function of ordinary number theory (see e.g. Apostol [1], Chapter 2). the summatory function of $\Lambda$ then satisfies

$$\bar{\Lambda}(m) = \sum_{\partial(a)=m} \Lambda(a) = \sum_{\substack{p \in \mathcal{P},\, r \geq 1 \\ \partial(p^r)=m}} \partial(p).$$

The properties of $\bar{\Lambda}$ developed below show that it is a counterpart of $N_m$, the number of points with coordinates in $\mathbb{F}_{q^m}$ of an algebraic curve $C$ defined over the finite field $\mathbb{F}_q$ (see Bombieri [2]). Firstly, we have $\bar{\Lambda}(0) = 0$, and

$$\bar{\Lambda}(n) = \sum_{r|n} r P(r), \quad n \geq 1,$$

and so, by the classical Möbius inversion formula of elementary number theory,

$$n P(n) = \sum_{r|n} \bar{\Lambda}(r) \mu(n/r), \quad n \geq 1,$$

where $\mu$ is the classical Möbius function on $\mathbb{N}$. The function $\bar{\Lambda}(n)$ of $n \geq 1$ is often technically easier to handle than $P(n)$ when one investigates problems involving the distribution of primes in an additive arithmetical semigroup, especially in the investigation of abstract prime number theorems. The functions $\bar{\Lambda}$ and $G$ satisfy the convolution equation

$$\bar{\Lambda} * G = LG, \tag{1.7}$$

which is an analogue of *Chebyshev's identity* in classical number theory.

An easy way to verify (1.7) is to first note that, for $a = p_1^{r_1} p_2^{r_2} \dots p_m^{r_m} \in \mathcal{G}$ where $p_i \in \mathcal{P}$ are distinct,

$$\partial(a) = \sum_{i=1}^{m} r_i \partial(p_i) = \sum_{i=1}^{m} \sum_{p_i^s | a} \Lambda(p_i^s) = \sum_{d|a} \Lambda(d).$$

(Thus the degree mapping $\partial = \Lambda *_1 \zeta$, where $*_1$ is the Dirichlet–type convolution on $\mathcal{G}$ and $\zeta$ is the constant function with $\zeta(b) = 1$ for $b \in \mathcal{G}$.) It follows that

$$\begin{aligned}
(LG)(n) &= nG(n) = \sum_{\partial(a)=n} \partial(a) = \sum_{\partial(a)=n} \sum_{d|a} \Lambda(d) \\
&= \sum_{\partial(a)=n} \sum_{cd=a} \Lambda(d) = \sum_{\partial(c)+\partial(d)=n} \Lambda(d) \\
&= \sum_{k=0}^{n} \sum_{\partial(c)=k} \sum_{\partial(d)=n-\partial(c)} \Lambda(d) \\
&= \sum_{k=0}^{n} G(k) \sum_{\partial(d)=n-k} \Lambda(d) = \sum_{k=0}^{n} G(k) \bar{\Lambda}(n-k),
\end{aligned}$$

which proves (1.7).

In terms of generating functions, (1.7) implies that

$$Z(y)\Lambda^{\#}(y) = \sum_{n=0}^{\infty} nG(n) y^n = yZ'(y)$$

or

$$\Lambda^{\#}(y) = yZ'(y)/Z(y).$$

It is this last equation which particularly brings out the abovementioned analogy of $\bar{\Lambda}(m)$ with the counting numbers $N_m$ for certain algebraic curves $C$.

From (1.7), we obtain also

$$L^2G = L\bar{\Lambda} * G + \bar{\Lambda} * LG.$$

Substitution of $LG = \bar{\Lambda} * G$ into the right-hand side yields

$$L^2G = \bar{\Lambda} * \bar{\Lambda} * G + L\bar{\Lambda} * G \tag{1.8}$$

which is an analogue of the *Selberg identity* of classical number theory (see e.g. Apostol [1], Chapter 2).

Lastly we note that the usefulness of $\Lambda$ in deriving asymptotic information about the numbers $P(n)$ (abstract prime theorems) within contexts which are fairly closely related to Axiom $\mathcal{A}^{\#}$ stems largely from the following simple proposition.

(3.1.7) PROPOSITION.[5] *If $G(n) \ll q^n k(n)$ for a constant $q > 1$ and a function $k(n) \ll n^{\alpha}$ for a constant $\alpha$, then*

$$P(m) = \frac{1}{m}\bar{\Lambda}(m) + O\left(q^{\frac{1}{2}m} k\left(\frac{m}{2}\right)\log m\right),$$

*and so*

$$P(m) \sim \frac{1}{m}q^m \textit{ if and only if } \bar{\Lambda}(m) \sim q^m \textit{ as } m \to \infty.$$

PROOF. Note that

$$\bar{\Lambda}(m) = mP(m) + \sum_{2 \le r | m} \frac{m}{r} P\left(\frac{m}{r}\right).$$

Therefore, since $P(r) \le G(r) \ll q^r k(r)$,

$$\begin{aligned}\bar{\Lambda}(m) &= mP(m) + O\left(mG\left(\frac{m}{2}\right)\sum_{r \le m}\frac{1}{r}\right) \\ &= mP(m) + O\left(mq^{\frac{1}{2}m} k\left(\frac{m}{2}\right)\log m\right). \qquad \square\end{aligned}$$

[5] The notation $\ll$ is used here as usual, as a replacement for $O(\ )$.

## 3.2 Chebyshev–Type Upper Bounds

We first consider *Chebyshev–type* upper bounds for $P(n)$, the distribution function of prime elements in $\mathcal{G}$. Such upper bounds are of interest for two reasons besides their easy proofs. As is well-known, a number of theorems in classical number theory (e.g. the Hardy–Ramanujan theorem on $\omega(n)$ and $\Omega(n)$) can be proved with the aid of the Chebyshev theorem and without appealing to the classical prime number theorem. A similar situation exists in the theory exposed in this monograph. Also, as we shall see from the discussion of this chapter, unlike the abstract prime number theorem, which requires rather restrictive conditions, the Chebyshev type upper bounds can be established under rather loose ones and hence holds in principle for a much larger variety of additive arithmetical semigroups. This makes it possible to prove many theorems in the following chapters under these looser conditions.

(3.2.1) THEOREM. (Chebyshev–type upper bounds) *Suppose there exist constants $A > 0$ and $q > 1$ such that*

$$\sum_{n=1}^{\infty} \sup_{n \leq m} \Big| G(m)q^{-m} - A \Big| < \infty. \tag{2.1}$$

*Then $\bar{\Lambda}(n) \ll q^n$ and $P(n) \ll q^n n^{-1}$.*

This theorem has the following direct corollary which is convenient to apply; for further reference, see Zhang [1,2].

(3.2.2) COROLLARY. *If there exist constants $A > 0$, $q > 1$, and $\gamma > 1$ such that*

$$G(n) = Aq^n + O(q^n n^{-\gamma}), \quad n = 1, 2, \ldots$$

*then $\bar{\Lambda}(n) \ll q^n$ and $P(n) \ll q^n n^{-1}$.*

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

PROOF. To prove Theorem 3.2.1, we need several lemmas. We first define an auxiliary function

$$Q_1(n) = \max\left\{\sup_{n\le m}\left|G(m)q^{-m} - A\right|, n^{-5/4}\right\}, \quad n \ge 1. \tag{2.2}$$

By (2.1),

$$\sum_{n=1}^{\infty} Q_1(n) < \infty. \tag{2.3}$$

Moreover, $Q_1(n)$ is non–negative and non–increasing.

(3.2.3) LEMMA. *If $Q_1(n)$ is a non–negative and non–increasing arithmetical function satisfying (2.3), then there exists an arithmetical function $Q(n)$ defined for $n \ge 0$ such that*

$$Q(n) \textit{ is non–increasing,} \tag{2.4}$$

$$Q(n) \ge Q_1(n) \textit{ for all } n \in \mathbb{N}, \tag{2.5}$$

$$\sum_{n=0}^{\infty} Q(n) < \infty, \tag{2.6}$$

$$Q(n) \le 4Q(2n). \tag{2.7}$$

PROOF. Define $Q(n)$ recursively by setting

$$Q(n) = \begin{cases} Q_1(1), & \text{for } 0 \le n \le 2, \\ \max\left\{Q_1(2^m), 4^{-1}Q(2^m)\right\}, & \text{for } 2^m < n \le 2^{m+1},\ m \in \mathbb{N}. \end{cases}$$

We now verify that this function satisfies each of the following conditions (1) – (4):

(1) $Q(n) \ge Q_1(n)$ (obvious).

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

(2) $Q(n)$ is non-increasing.

Here, first note that $Q(n)$ is constant for $2^m < n \leq 2^{m+1}$. If $1 \leq n_1 \leq 2 < n_2 \leq 2^2$, then

$$Q(n_2) = \max\left\{Q_1(2), 4^{-1}Q(2)\right\} \leq Q(1) = Q(n_1).$$

If $2^{m-1} < n_1 \leq 2^m < n_2 \leq 2^{m+1}$, then

$$Q(n_2) = \max\left\{Q_1(2^m), 4^{-1}Q(2^m)\right\} \leq Q(2^m) = Q(n_1),$$

since, by (1), $Q_1(2^m) \leq Q(2^m)$.

(3) $Q(n) \leq 4Q(2n)$.

For (3) note that, if $1 \leq n \leq 2$, we have $2 \leq 2n \leq 4$, and if $2n = 2$, then $Q(n) = Q(2n) = Q_1(1)$, and we have nothing to show. If $2 < 2n \leq 4$, we have

$$Q(2n) = \max\left\{Q_1(2), 4^{-1}Q(2)\right\} \geq 4^{-1}Q(2) = 4^{-1}Q(n).$$

For $2^m < n \leq 2^{m+1}$, $m \geq 1$, we have $2^{m+1} < 2n \leq 2^{m+2}$, and hence

$$\begin{aligned} Q(2n) &= \max\left\{Q_1(2^{m+1}), 4^{-1}Q(2^{m+1})\right\} \\ &\geq 4^{-1}Q(2^{m+1}) = 4^{-1}Q(n). \end{aligned}$$

(4) $\sum_{n=0}^{\infty} Q(n) < \infty$.

To verify (4), note that $\sum_{n=0}^{\infty} Q(n) < \infty$ if and only if $\sum_{m=1}^{\infty} Q(2^m)2^m < \infty$, since $Q(n)$ is non-increasing. There are two distinct cases that we need to consider separately:

Case I. $4^{-1}Q(2^m) \geq Q_1(2^m)$ for all $m \geq m_0$. In this case,

$$Q(2^{m_0+1}) = \max\left\{Q_1(2^{m_0}), 4^{-1}Q(2^{m_0})\right\} = 4^{-1}Q(2^{m_0}).$$

By induction, for all $m \geq m_0 + 1$, we have

$$Q(2^m) = 4^{-(m-m_0)} Q(2^{m_0}).$$

Therefore

$$\begin{aligned} \sum_{m=m_0+1}^{\infty} Q(2^m) 2^m &= \sum_{m=m_0+1}^{\infty} 4^{-(m-m_0)} Q(2^{m_0}) 2^m \\ &= Q(2^{m_0}) 2^{m_0}. \end{aligned}$$

Case II. There exists an infinite sequence $m_1 < m_2 < \cdots < m_k < m_{k+1} < \cdots$ such that $Q_1(2^{m_k}) > 4^{-1} Q(2^{m_k})$, and $Q_1(2^m) \leq 4^{-1} Q(2^m)$ for all $m \notin \{m_k : k = 1, 2, \ldots\}$. In this case, we can deduce that

$$\sum_{m=m_k+1}^{m_{k+1}} Q(2^m) 2^m \leq 4 Q_1(2^{m_k}) 2^{m_k}.$$

Actually, if $m_{k+1} = m_k + 1$, then the left-hand side equals

$$\begin{aligned} Q(2^{m_k+1}) 2^{m_k+1} &= \max \left\{ Q_1(2^{m_k}), 4^{-1} Q(2^{m_k}) \right\} 2^{m_k+1} \\ &= Q_1(2^{m_k}) 2^{m_k+1}. \end{aligned}$$

Therefore we consider $m_k < m_k + 2 \leq m_{k+1}$. We have

$$Q(2^{m_k+1}) = Q_1(2^{m_k}),$$

and

$$\begin{aligned} Q(2^{m_k+2}) &= \max \left\{ Q_1(2^{m_k+1}), 4^{-1} Q(2^{m_k+1}) \right\} \\ &= 4^{-1} Q(2^{m_k+1}) = 4^{-1} Q_1(2^{m_k}). \end{aligned}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

By induction, for all $m \in [m_k + 1, m_{k+1}]$, we have

$$Q(2^m) = 4^{-(m-m_k)+1} Q_1(2^{m_k}).$$

It follows that

$$\begin{aligned} \sum_{m=m_k+1}^{m_{k+1}} Q(2^m)2^m &= Q_1(2^{m_k}) \sum_{m=m_k+1}^{m_{k+1}} 4^{-(m-m_k)+1} 2^m \\ &= Q_1(2^{m_k}) 2^{m_k+2} \sum_{\ell=1}^{m_{k+1}-m_k} 2^{-\ell} \\ &\leq 4Q_1(2^{m_k})2^{m_k}. \end{aligned}$$

Thus we obtain

$$\begin{aligned} \sum_{k=1}^{\infty} \sum_{m=m_k+1}^{m_{k+1}} Q(2^m)2^m &\leq 4\sum_{k=1}^{\infty} 2^{m_k} Q_1(2^{m_k}) \\ &\leq 8\sum_{k=1}^{\infty} \sum_{n=2^{m_{k-1}}+1}^{2^{m_k}} Q_1(n) \\ &\leq 8\sum_{n=1}^{\infty} Q_1(n) < \infty, \end{aligned}$$

since $Q_1(n)$ is non–increasing and $2^{m_k} - 2^{m_{k-1}} \geq 2^{m_k - 1}$. □

(3.2.4) LEMMA. *Assume (2.4), (2.6) and (2.7). Then the function $Q(n)$ has the following properties:*

$$\sum_{t=0}^{n} Q(t)Q(n-t) \ll Q(n), \tag{2.8}$$

$$Q(n) = o(n^{-1}). \tag{2.9}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

PROOF. We have

$$\begin{aligned}\sum_{t=0}^{n} Q(t)Q(n-t) &\leq 2 \sum_{0\leq t\leq \frac{n}{2}} Q(t)Q(n-t)\\ &\leq 2Q\left(n-\left[\frac{n}{2}\right]\right) \sum_{0\leq t\leq \frac{n}{2}} Q(t)\\ &\ll Q\left(n-\left[\frac{n}{2}\right]\right) \ll Q(n),\end{aligned}$$

by (2.4), (2.6), and (2.7). Moreover, by (2.6) and (2.7),

$$nQ(2n) \leq Q(n+1) + \cdots + Q(2n) < \varepsilon/2$$

for $n \geq n_0$ sufficiently large. Thus (2.9) follows. □

We now define arithmetical functions $U$ and $M$ by setting

$$U(n) = \begin{cases} 1, & \text{for } n = 0,\\ -q^{n_0}, & \text{for } n = n_0,\\ 0, & \text{otherwise,}\end{cases} \tag{2.10}$$

and

$$M(n) = \begin{cases} 0, & \text{if } n \leq n_0,\\ q^n Q(n), & \text{if } n > n_0,\end{cases} \tag{2.11}$$

where $n_0$ is a positive integer to be specified later and where $Q(n)$ is the function defined in Lemma 3.2.3.

(3.2.5) LEMMA. *Assume (2.1). Let $Q(n)$ be the function defined in Lemma 3.2.3 with $Q_1(n)$ defined in (2.2). Then, for fixed $n_0$ sufficiently large, the arithmetical function $V := G*U*M$ is non-negative and $V(n) \to \infty$ as $n \to \infty$.*

PROOF. We first note that $G * M(n) = 0$ and hence $V(n) = 0$ if $n \leq n_0$. For $n_0 < n \leq 2n_0$, it is easy to see that

$$V(n) = G * M(n) - q^{n_0} G * M(n - n_0) = G * M(n) \geq 0.$$

Therefore we may assume that $n > 2n_0$. Write

$$G(n) = Aq^n + R_n = q^n(A + r_n), \text{ for } n \geq 1.$$

By (2.2) and (2.5), $|r_n| \leq Q_1(n) \leq Q(n)$. Then we have

$$\begin{aligned}
V(n) &= \sum_{t=0}^{n-n_0-1} \left( \sum_{m=0}^{t} U(t-m)G(m) \right) M(n-t) \\
&= \sum_{t=0}^{n-n_0-1} G(t)M(n-t) - q^{n_0} \sum_{t=n_0}^{n-n_0-1} G(t-n_0)M(n-t) \\
&= q^n \left( Q(n) + \sum_{t=1}^{n-n_0-1} (A + r_t)Q(n-t) \right. \\
&\qquad \left. - Q(n-n_0) - \sum_{t=n_0+1}^{n-n_0-1} (A + r_{t-n_0})Q(n-t) \right) \\
&\geq q^n \left( A \sum_{t=1}^{n-n_0-1} Q(n-t) - \sum_{t=1}^{n-n_0-1} Q(t)Q(n-t) \right. \\
&\qquad - Q(n-n_0) - A \sum_{t=n_0+1}^{n-n_0-1} Q(n-t) \\
&\qquad \left. - \sum_{t=n_0+1}^{n-n_0-1} Q(t-n_0)Q(n-t) \right) \\
&\geq Aq^n \sum_{m=n-n_0}^{n-1} Q(m) - q^n \sum_{t=1}^{n-n_0-1} Q(t)Q(n-t)
\end{aligned}$$

$$- q^n \sum_{t=1}^{n-2n_0-1} Q(t)Q(n-n_0-t) - q^n Q(n-n_0)$$

$$\geq \; Aq^n n_0 Q(n) - (5K+4)q^n Q(n)$$

since, by (2.8) and (2.7),

$$\sum_{t=1}^{n-n_0-1} Q(t)Q(n-t) \leq KQ(n)$$

and

$$\sum_{t=1}^{n-2n_0-1} Q(t)Q(n-n_0-t) \leq KQ(n-n_0) \leq 4KQ(n)$$

for $n > 2n_0$. We now choose $n_0$ satisfying

$$An_0 > 2(5K+4)$$

and arrive at

$$V(n) \geq \frac{1}{2} An_0 q^n Q(n).$$

Thus $V(n) \geq 0$ and $V(n) \to \infty$ as $n \to \infty$ by (2.5) and (2.2). □

Proof of Theorem 3.2.1 It suffices to show that $\bar{\Lambda}(n) \ll q^n$. We begin with the convolution equation (1.7)

$$\bar{\Lambda} * G = LG.$$

Convolving both sides of this equation by $U * M$, where the arithmetical functions $U$ and $M$ are defined in (2.10) and (2.11), respectively, we obtain

$$\bar{\Lambda} * G * U * M(n) = LG * U * M(n). \tag{2.12}$$

We then show that the magnitude of the right-hand side of (2.12) is $O(q^n)$. Actually we have

$$\begin{aligned} LG * U(n) &= nG(n) - (n-n_0)G(n-n_0)q^{n_0} \\ &= An_0q^n + nq^n r_n - (n-n_0)q^n r_{n-n_0} \\ &\ll q^n, \end{aligned}$$

since $|r_n| \leq Q(n) = o(n^{-1})$, by (2.9). Therefore,

$$\begin{aligned} LG * U * M(n) &= \sum_{t=n_0+1}^{n} O(q^{n-t})q^t Q(t) \\ &= O(q^n) \qquad (2.13) \end{aligned}$$

by (2.6). Now, from (2.12) and (2.13), for $n$ sufficiently large,

$$\bar{\Lambda}(n - n_1)V(n_1) \leq \bar{\Lambda} * V(n) \leq Kq^n,$$

where $V = G * U * M$ is non–negative by Lemma 3.2.5 ($\bar{\Lambda}$ is non–negative). This implies that $\bar{\Lambda}(n - n_1) \leq Kq^n$, i.e., $\bar{\Lambda}(n) \leq Kq^{n+n_1}$ since for fixed $n_1$, sufficiently large, $V(n_1) \geq 1$ by Lemma 3.2.5. □

Having proved Chebyshev–type upper bounds, it is then natural to ask for Chebyshev–type lower bounds. To answer this question, a consequence of Theorem 5.4.1 of Chapter 5 below will show that a lower estimate $\bar{\Lambda}(n) \gg q^n$ is, in the general case, essentially equivalent to the abstract prime number theorem, and hence requires the same restrictive conditions as the latter does. This indicates a major divergence of the theory of additive arithmetical semigroups from classical number theory.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

## 3.3 Mertens–Type Asymptotic Estimates and Prime Divisor Functions

In this section we consider some consequences of Chebyshev–type upper bounds. We first deduce *Mertens–type* asymptotic estimates with the aid of those bounds. These estimates have many uses. In particular, we shall apply them to the investigation of the *prime divisor* functions $\omega$ and $\Omega$ on $\mathcal{G}$ such that $\omega(a)$ equals the total number of different primes dividing $a \in \mathcal{G}$, while $\Omega(a)$ counts these primes together with their *multiplicity* relative to $a$.

### 3.3.1 Mertens–type estimates (cf. Zhang [3])

(3.3.1) THEOREM. *Suppose there exist constants $A > 0$ and $q > 1$ such that*

$$\sum_{n=1}^{\infty} \sup_{n \le m} \left| G(m) q^{-m} - A \right| < \infty. \tag{3.1}$$

*Then*

$$\sum_{m=1}^{n} \bar{\Lambda}(m) q^{-m} = n + O(1). \tag{3.2}$$

PROOF. As in the proof of Theorem 3.2.1, we begin with the convolution equation (1.7)

$$\bar{\Lambda} * G = LG,$$

i.e.,

$$\bar{\Lambda}(n) + \sum_{1 \le s \le n-1} \bar{\Lambda}(s) G(n-s) = nG(n), \quad n \ge 1. \tag{3.3}$$

We write again

$$G(n) = q^n (A + r_n), \quad n \ge 1.$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Dividing both sides of (3.3) by $q^n$, we obtain

$$\frac{\bar{\Lambda}(n)}{q^n} + A \sum_{1 \leq s \leq n-1} \frac{\bar{\Lambda}(s)}{q^s} + \sum_{1 \leq s \leq n-1} \frac{\bar{\Lambda}(s)}{q^s} r_{n-s} = nA + r_n,$$

and hence

$$\sum_{1 \leq s \leq n} \frac{\bar{\Lambda}(s)}{q^s} = n + O(1),$$

since $\bar{\Lambda}(n) \ll q^n$, by Theorem 3.2.1, and $\sum_{n=1}^{\infty} |r_n| < \infty$, by (3.1). □

(3.3.2) THEOREM. *Assume (3.1). Then*

$$\sum_{\partial(p) \leq n} q^{-\partial(p)} = \sum_{1 \leq m \leq n} P(m) q^{-m} = \log n + c + O(n^{-1}), \tag{3.4}$$

*where c is a constant.*

PROOF. We have $\bar{\Lambda}(n) \ll q^n$, and the sum

$$S(n) := \sum_{k=1}^{n} \frac{\bar{\Lambda}(k)}{q^k} = n + O(1), \tag{3.5}$$

by Theorem 3.3.1. Then, for the classical Möbius function $\mu$ on $\mathbb{N}$,

$$\begin{aligned}
\sum_{1 \leq m \leq n} P(m) q^{-m} &= \sum_{m=1}^{n} \left( \frac{1}{m} \sum_{r|m} \bar{\Lambda}(r) \mu\left(\frac{m}{r}\right) \right) q^{-m} \\
&= \sum_{r=1}^{n} \bar{\Lambda}(r) \sum_{1 \leq s \leq \frac{n}{r}} \frac{1}{sr} \mu(s) q^{-sr} \\
&= \sum_{r=1}^{n} \frac{\bar{\Lambda}(r)}{r} q^{-r} + \sum_{r=1}^{n} \frac{\bar{\Lambda}(r)}{r} \sum_{2 \leq s \leq \frac{n}{r}} \frac{\mu(s)}{s} q^{-sr} \\
&= S_1 + S_2,
\end{aligned}$$

say. By (3.5), we have

$$\begin{aligned} S_1 &= \sum_{r=1}^{n} \frac{S(r)-S(r-1)}{r} = \frac{S(n)}{n} + \sum_{r=1}^{n-1} \frac{S(r)}{r(r+1)} \\ &= 1 + O(n^{-1}) + \sum_{r=1}^{n-1} \frac{1}{r+1} + \sum_{r=1}^{n-1} \frac{O(1)}{r(r+1)} \\ &= \log n + c_1 + O(n^{-1}), \end{aligned}$$

where

$$c_1 = \gamma + \sum_{r=1}^{\infty} \frac{1}{r(r+1)} \left( \sum_{k=1}^{r} \bar{\Lambda}(k) q^{-k} - r \right)$$

and $\gamma$ is the classical Euler constant. To obtain an asymptotic formula for $S_2$, let

$$d_r := \sum_{s=2}^{\infty} \frac{\mu(s)}{s} q^{-sr}.$$

Then

$$d_r \ll \sum_{s=2}^{\infty} \frac{q^{-sr}}{s} \ll q^{-2r}. \tag{3.6}$$

Hence

$$\sum_{2 \le s \le \frac{n}{r}} \frac{\mu(s)}{s} q^{-sr} = d_r + O(rq^{-n}n^{-1}).$$

Thus we obtain

$$S_2 = \sum_{r=1}^{n} \frac{\bar{\Lambda}(r)}{r} d_r + O\left( n^{-1} q^{-n} \sum_{r=1}^{n} \bar{\Lambda}(r) \right). \tag{3.7}$$

By (3.6)

$$\begin{aligned} \sum_{r=1}^{n} \frac{\bar{\Lambda}(r)}{r} d_r &= c_2 - \sum_{r=n+1}^{\infty} \frac{\bar{\Lambda}(r)}{r} d_r \\ &= c_2 + O\left( \sum_{r=n+1}^{\infty} \frac{q^{-r}}{r} \right) \\ &= c_2 + O(n^{-1}), \end{aligned}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

where

$$c_2 = \sum_{r=1}^{\infty} \frac{\bar{\Lambda}(r)}{r} \sum_{s=2}^{\infty} \frac{\mu(s)}{s} q^{-sr}.$$

Moreover, the last sum in (3.7) is

$$\ll \sum_{r=1}^{n} q^{r} \ll q^{n}.$$

It follows that

$$S_2 = c_2 + O(n^{-1}).$$

Then (3.4) follows with $c = c_1 + c_2$. □

(3.3.3) THEOREM. *Assume (3.1). Then*

$$\sum_{\partial(p)\leq n} \partial(p) q^{-\partial(p)} = \sum_{1\leq m\leq n} mP(m)q^{-m} = n + O(1). \tag{3.8}$$

PROOF. As in the proof of Theorem 3.3.2, we have

$$\begin{aligned} \sum_{1\leq m\leq n} mP(m)q^{-m} &= \sum_{r=1}^{n} \bar{\Lambda}(r) \sum_{1\leq s\leq \frac{n}{r}} \mu(s) q^{-sr} \\ &= \sum_{r=1}^{n} \bar{\Lambda}(r) q^{-r} + \sum_{r=1}^{n} \bar{\Lambda}(r) \sum_{2\leq s\leq \frac{n}{r}} \mu(s) q^{-sr} \\ &= S_1 + S_2, \end{aligned}$$

say. By (3.5),

$$S_1 = n + O(1).$$

Moreover, since

$$\sum_{2\leq s\leq \frac{n}{r}} \mu(s) q^{-sr} \ll q^{-2r},$$

we have

$$S_2 \ll \sum_{r=1}^{n} \bar{\Lambda}(r) q^{-2r} \ll \sum_{r=1}^{n} q^{-r} \ll 1.$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Then (3.8) follows. □

(3.3.4) THEOREM. *Assume (3.1). Then*

$$\prod_{\partial(p)\leq n}\left(1-q^{-\partial(p)}\right)=\frac{c_3}{n}\left(1+O(n^{-1})\right), \qquad (3.9)$$

*where $c_3$ is a positive constant.*

PROOF. The left–hand side equals

$$\begin{aligned}
&\exp\left\{\sum_{\partial(p)\leq n}\log\left(1-q^{-\partial(p)}\right)\right\}\\
&\quad=\exp\left\{\sum_{\partial(p)\leq n}\left(-q^{-\partial(p)}+O(q^{-2\partial(p)})\right)\right\}\\
&\quad=\exp\left\{-\log n-c_1+O(n^{-1})+O\left(\sum_{\partial(p)\leq n}q^{-2\partial(p)}\right)\right\}
\end{aligned}$$

by (3.4). The last sum equals

$$\begin{aligned}
\sum_{1\leq m\leq n}P(m)q^{-2m} &= c_2+\sum_{m>n}q^{-2m}P(m)\\
&= c_2+O\left(\frac{q^{-n}}{n}\right),
\end{aligned}$$

where

$$c_2:=\sum_{m=1}^{\infty}P(m)q^{-2m}\ll\sum_{m=1}^{\infty}\frac{q^{-m}}{m}.$$

Thus (3.9) follows. □

The following lemma gives some elementary estimates which will be used repeatedly later.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

(3.3.5) LEMMA.

*(i) Let $q > 1$ and $\gamma > 0$. Then*

$$\sum_{1\le m\le n} q^m m^{-\gamma} = O(q^n n^{-\gamma}). \tag{3.10}$$

*(ii) Suppose $P(m) \ll q^m m^{-1}$ with $q > 1$. Then, for any positive integer $n$,*

$$\sum_{1\le m\le n} P(m) = O(q^n n^{-1}). \tag{3.11}$$

PROOF. We first have

$$\begin{aligned}\sum_{1\le m\le n} q^m m^{-\gamma} &\ll q^{\frac{n}{2}} \sum_{1\le m\le \frac{n}{2}} m^{-\gamma} + n^{-\gamma} \sum_{\frac{n}{2}<m\le n} q^m \\ &\ll q^{\frac{n}{2}} \left(1 + n^{-\gamma+1}\right) + n^{-\gamma} q^n \\ &\ll q^n n^{-\gamma}.\end{aligned}$$

Thus (3.11) is a direct consequence of (3.10) with $\gamma = 1$. □.

### 3.3.2 Prime divisor functions

As an application of the above Mertens–type asymptotic estimates, we investigate some "statistical" properties of the prime divisor functions $\omega$ and $\Omega$ on an additive arithmetical semigroup $\mathcal{G}$, such that (for $a \in \mathcal{G}$) $\omega(a)$ and $\Omega(a)$ denote the number of distinct prime divisors of $a$ and the total number of prime divisors of $a$ with multiplicity counted, respectively.

*Remark.* These two functions were investigated in [ANAL], with similar conclusions to those below, within the general context of Axiom $A^{\#}$. However the following two theorems under the very weak condition (3.12) are proved for the first time in this monograph, and the proofs have not been published before. The proofs are simpler.

(3.3.6) THEOREM. *Suppose there exist constants $A > 0$, $q > 1$, and $\gamma > 1$, such that*

$$G(n) = Aq^n + O\left(q^n n^{-\gamma}\right). \tag{3.12}$$

*Then*

$$\sum_{\partial(a)=n} \omega(a) = q^n\left(A\log n + c_1 + O(n^{-1})\right) \tag{3.13}$$

*and*

$$\sum_{\partial(a)=n} \Omega(a) = q^n\left(A\log n + c_2 + O(n^{-1})\right), \tag{3.14}$$

*where $c_1$ and $c_2$ are constants.*

PROOF. We have

$$\begin{aligned}\sum_{\partial(a)=n} \omega(a) &= \sum_{\partial(a)=n}\sum_{p|a} 1 = \sum_{\partial(p)\leq n}\sum_{\substack{\partial(a)=n\\ p|a}} 1\\ &= \sum_{\partial(p)\leq n}\sum_{\partial(b)=n-\partial(p)} 1 = \sum_{\partial(p)\leq n} G(n-\partial(p))\\ &= \sum_{1\leq m\leq n} G(n-m)P(m)\end{aligned}$$

and hence we may write

$$\begin{aligned}\sum_{\partial(a)=n} \omega(a) &= P(n) + \sum_{1\leq m\leq n-1} Aq^{n-m}\frac{\bar{\Lambda}(m)}{m}\\ &\quad + \sum_{1\leq m\leq n-1}\left(G(n-m) - Aq^{n-m}\right)\frac{\bar{\Lambda}(m)}{m}\end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

$$
\begin{aligned}
&+\sum_{1\le m\le n-1} G(n-m)\left(P(m)-\frac{\bar{\Lambda}(m)}{m}\right)\\
=\;& P(n)+S_1+S_2+S_3, \qquad (3.15)
\end{aligned}
$$

say. By (3.2),

$$S(n):=\sum_{m=1}^{n}\bar{\Lambda}(m)q^{-m}=n+O(1).$$

Hence

$$
\begin{aligned}
\sum_{1\le m\le n-1} q^{-m}\frac{\bar{\Lambda}(m)}{m} &= \sum_{1\le m\le n-1}\frac{S(m)-S(m-1)}{m}\\
&= \frac{S(n-1)}{n-1}+\sum_{1\le m\le n-2}\frac{S(m)}{m(m+1)}\\
&= \sum_{0\le m\le n-2}\frac{1}{m+1}+\sum_{1\le m\le n-2}\frac{S(m)-m}{m(m+1)}+O(n^{-1})\\
&= \log n+c_3+O(n^{-1}),
\end{aligned}
$$

where

$$c_3=\gamma+\sum_{m=1}^{\infty}\frac{S(m)-m}{m(m+1)}$$

and $\gamma$ is the Euler constant, since

$$\sum_{m\ge n-1}\frac{S(m)-m}{m(m+1)}=\sum_{m\ge n-1}\frac{O(1)}{m(m+1)}=O(n^{-1}).$$

Then

$$
\begin{aligned}
S_1 &= \sum_{1\le m\le n-1} Aq^{n-m}\frac{\bar{\Lambda}(m)}{m}\\
&= Aq^n\left(\log n+c_3+O(n^{-1})\right). \qquad (3.16)
\end{aligned}
$$

Also, by (3.12) and $\bar{\Lambda}(n) \ll q^n$,

$$S_2 = q^n \sum_{1 \le m \le n-1} O\left(\frac{1}{m}\frac{1}{(n-m)^\gamma}\right) = q^n O(n^{-1}), \tag{3.17}$$

since

$$\sum_{\frac{n}{2} < m \le n-1} \frac{1}{(n-m)^\gamma m} \ll n^{-1} \sum_{\frac{n}{2} < m \le n-1} \frac{1}{(n-m)^\gamma} \ll n^{-1}$$

and

$$\sum_{1 \le m \le \frac{n}{2}} \frac{1}{(n-m)^\gamma m} \ll n^{-\gamma} \sum_{1 \le m \le \frac{n}{2}} \frac{1}{m} \ll n^{-\gamma} \log n \ll n^{-1},$$

for $\gamma > 1$.

Finally,

$$\begin{aligned} S_3 &= \sum_{1 \le m \le n-1} \left(Aq^{n-m} + O\left(q^{n-m}(n-m)^{-\gamma}\right)\right)\left(P(m) - \frac{\bar{\Lambda}(m)}{m}\right) \\ &= Aq^n \sum_{1 \le m \le n-1} q^{-m}\left(P(m) - \frac{\bar{\Lambda}(m)}{m}\right) \\ &\quad + q^n O\left(\sum_{1 \le m \le n-1} \frac{1}{(n-m)^\gamma} q^{-m/2}\right) \\ &= q^n \left(Ac_4 + O(n^{-1})\right), \end{aligned} \tag{3.18}$$

where

$$c_4 = \sum_{m=1}^{\infty} q^{-m}\left(P(m) - \frac{\bar{\Lambda}(m)}{m}\right),$$

since

$$\sum_{1 \le m \le \frac{n}{2}} \frac{1}{(n-m)^\gamma} q^{-\frac{m}{2}} \ll n^{-\gamma}$$

and

$$\sum_{\frac{n}{2} < m \le n-1} \frac{1}{(n-m)^\gamma} q^{-\frac{m}{2}} \ll q^{-\frac{n}{4}}.$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Thus (3.13) follows from (3.15), (3.16), (3.17) and (3.18).

We then turn to the function $\Omega$. Note that

$$\begin{aligned}\sum_{\partial(a)=n} \Omega(a) &= \sum_{\partial(a)=n} \sum_{\substack{r\geq 1,\, p\in\mathcal{P} \\ p^r|a}} 1 = \sum_{\substack{r\geq 1,\, p\in\mathcal{P} \\ r\partial(p)\leq n}} \sum_{\substack{\partial(a)=n \\ p^r|a}} 1 \\ &= \sum_{\partial(a)=n} \omega(a) + \sum_{\substack{r\geq 2,\, p\in\mathcal{P} \\ r\partial(p)\leq n}} G(n - r\partial(p)). \qquad (3.19)\end{aligned}$$

The last sum can be written in the form

$$\sum_{\substack{r\geq 2,\, m\geq 1 \\ rm\leq n}} G(n-rm)P(m) = Aq^n \sum_{\substack{r\geq 2,\, m\geq 1 \\ rm\leq n}} q^{-rm}P(m)$$

$$+q^n \sum_{\substack{r\geq 2, m\geq 1 \\ rm<n}} O\left(\frac{q^{-(r-1)m}}{(n-rm)^{\gamma}m}\right) + \sum_{\substack{m|n \\ 1\leq m\leq \frac{n}{2}}} P(m).$$

We have

$$\sum_{\substack{r\geq 2, m\geq 1 \\ rm\leq n}} q^{-rm}P(m) = c_5 + O\left(nq^{-\frac{n}{2}}\right),$$

where

$$c_5 = \sum_{r\geq 2, m\geq 1} q^{-rm}P(m) = \sum_{m=1}^{\infty} q^{-2m}(1-q^{-m})^{-1}P(m),$$

since

$$\sum_{\substack{r\geq 2, m\geq 1 \\ rm\geq n}} q^{-rm}P(m) \ll \sum_{\substack{r\geq 2, m\geq 1 \\ rm\geq n}} q^{-(r-1)m}$$

$$= \sum_{r\geq 2} \sum_{m\geq \max\left\{1, \frac{n}{r}\right\}} q^{-(r-1)m}$$

$$\ll \sum_{r\geq 2} q^{-(r-1)\max\left\{1, \frac{n}{r}\right\}}$$

$$\begin{aligned}
&= \sum_{r\geq n} q^{-(r-1)} + \sum_{2\leq r<n} q^{-(r-1)\frac{n}{r}} \\
&\ll q^{-n} + \sum_{2\leq r<n} q^{-n+\frac{n}{r}} \\
&\ll q^{-n} + q^{-\frac{n}{2}} n.
\end{aligned}$$

Moreover, we have

$$\begin{aligned}
\sum_{\substack{r\geq 2, m\geq 1\\ rm\leq \frac{n}{2}}} O\left(\frac{q^{-(r-1)m}}{(n-rm)^{\gamma} m}\right) &\ll n^{-\gamma} \sum_{r\geq 2, m\geq 1} q^{-(r-1)m} \\
&\ll n^{-\gamma} \sum_{r\geq 2} q^{-(r-1)} \ll n^{-\gamma},
\end{aligned}$$

and

$$\begin{aligned}
\sum_{\substack{r\geq 2, m\geq 1\\ \frac{n}{2}<rm<n}} O\left(\frac{q^{-(r-1)m}}{(n-rm)^{\gamma} m}\right) &\ll \sum_{2\leq r<n} \frac{r}{n} q^{-(r-1)\frac{n}{2r}} \\
&\leq \sum_{2\leq r<n} \frac{r}{n} q^{-\frac{n}{4}} \ll q^{-\frac{n}{4}} n.
\end{aligned}$$

Hence

$$\sum_{\substack{r\geq 2, m\geq 1\\ rm<n}} O\left(\frac{q^{-(r-1)m}}{(n-rm)^{\gamma} m}\right) \ll n^{-\gamma}.$$

Finally,

$$\sum_{\substack{m|n\\ 1\leq m\leq \frac{n}{2}}} P(m) \ll \sum_{1\leq m\leq \frac{n}{2}} q^{m} \ll q^{\frac{n}{2}}.$$

Therefore, the last sum in (3.19) equals

$$q^{n}\left(Ac_{5} + O(n^{-\gamma})\right)$$

and (3.14) follows from (3.13) and (3.19). □

From Theorem 3.3.6, the mean– or average–values of $\omega$ and $\Omega$ for elements of degree $n$ are

$$\frac{1}{G(n)} \sum_{\partial(a)=n} \omega(a) = \log n + \frac{c_1}{A} + O(n^{-1}),$$

and

$$\frac{1}{G(n)} \sum_{\partial(a)=n} \Omega(a) = \log n + \frac{c_2}{A} + O(n^{-1}),$$

respectively.

We next consider an analogue of a theorem of Hardy and Ramanujan on the classical functions $\omega(n)$ and $\Omega(n)$ of $n \in \mathbb{N}$.

(3.3.7) THEOREM. *Assume (3.12). Let $f(a)$ denote $\omega(a)$ or $\Omega(a)$. Then, for any fixed $\delta > 0$,*

$$\#\left\{a : \partial(a) = n,\ |f(a) - \log n| \geq (\log n)^{\frac{1}{2}+\delta}\right\} = o(G(n)).$$

PROOF. Note that

$$\begin{aligned}&\left\{a : \partial(a) = n,\ |\Omega(a) - \log n| \geq (\log n)^{\frac{1}{2}+\delta}\right\}\\ &\quad\subseteq \left\{a : \partial(a) = n,\ |\omega(a) - \log n| \geq (\log n)^{\frac{1}{2}+\frac{\delta}{2}}\right\}\\ &\quad\cup \left\{a : \partial(a) = n,\ \Omega(a) - \omega(a) \geq (\log n)^{\frac{1}{2}+\frac{\delta}{2}}\right\}\end{aligned}$$

for $n \geq n_0$ sufficiently large. By Theorem 3.3.6,

$$\sum_{\partial(a)=n} (\Omega(a) - \omega(a)) \ll q^n,$$

and hence

$$\begin{aligned}
&\#\left\{a:\, \partial(a)=n,\, \Omega(a)-\omega(a)\geq (\log n)^{\frac{1}{2}+\frac{\delta}{2}}\right\}\\
&\quad\leq (\log n)^{-\frac{1}{2}-\frac{\delta}{2}}\sum_{\partial(a)=n}(\Omega(a)-\omega(a)) \ll q^n(\log n)^{-\frac{1}{2}-\frac{\delta}{2}}\\
&\quad= o(G(n)).
\end{aligned}$$

The stated conclusion for $\Omega$ is a direct consequence of that for $\omega$. We need only prove the theorem for $\omega$.

Now consider

$$\begin{aligned}
\sum_{\partial(a)=n}(\omega(a))^2 &= \sum_{\partial(a)=n}\omega(a)\sum_{p|a}1\\
&= \sum_{\partial(p)\leq n}\sum_{\substack{\partial(a)=n\\ p|a}}\omega(a) = \sum_{\partial(p)\leq n}\sum_{\partial(b)=n-\partial(p)}\omega(pb).
\end{aligned}$$

Since $\omega(b)\leq\omega(pb)\leq\omega(b)+1$, we have

$$\sum_{\partial(p)\leq n}\sum_{\partial(b)=n-\partial(p)}\omega(b)\leq\sum_{\partial(a)=n}(\omega(a))^2,$$

and

$$\begin{aligned}
\sum_{\partial(a)=n}(\omega(a))^2 &\leq \sum_{\partial(p)\leq n}\sum_{\partial(b)=n-\partial(p)}(\omega(b)+1)\\
&= \sum_{\partial(p)\leq n}\sum_{\partial(b)=n-\partial(p)}\omega(b)+\sum_{1\leq m\leq n}G(n-m)P(m)\\
&= \sum_{\partial(p)\leq n}\sum_{\partial(b)=n-\partial(p)}\omega(b)+O(q^n\log n),
\end{aligned}$$

by (3.4). Hence

$$\sum_{\partial(a)=n}(\omega(a))^2 = \sum_{\partial(p)\leq n}\sum_{\partial(b)=n-\partial(p)}\omega(b)+O(q^n\log n)$$

$$= \sum_{\partial(pp')\leq n} G(n-\partial(pp')) + O(q^n \log n).$$

We have

$$\begin{aligned}\sum_{\partial(pp')\leq n} G(n-\partial(pp')) &= \sum_{\partial(pp')=n} 1 + Aq^n \sum_{\partial(pp')<n} q^{-\partial(pp')} \\ &\quad +q^n \sum_{\partial(pp')<n} O\left(q^{-\partial(pp')}(n-\partial(pp'))^{-\gamma}\right). \quad (3.20)\end{aligned}$$

By Theorem 3.2.1, the first sum on the right–hand side of (3.20) equals

$$\begin{aligned}\sum_{\partial(p)+\partial(p')=n} 1 &= \sum_{m\leq n-1} P(n-m)P(m) \\ &\ll q^n \sum_{m\leq n-1} \frac{1}{(n-m)m} \ll q^n \frac{\log n}{n}.\end{aligned}$$

Applying (3.4) twice, the second sum on the right–hand side of (3.20) equals

$$\begin{aligned}&\sum_{\partial(p)<n} \sum_{\partial(p')<n-\partial(p)} q^{-\partial(p)-\partial(p')} \\ &= \sum_{\partial(p)\leq n-2} q^{-\partial(p)} \left(\log\left(n-\partial(p)-1\right) + O(1)\right) \\ &= \sum_{m\leq n-2} q^{-m} P(m) \log(n-m-1) + O(\log n).\end{aligned}$$

We have

$$\begin{aligned}&\sum_{m\leq n-2} q^{-m} P(m) \log(n-m-1) \\ &= \sum_{m\leq n-2} q^{-m} \log(n-m-1) \left(\frac{\bar{\Lambda}(m)}{m} + O\left(\frac{q^{\frac{m}{2}}}{m}\right)\right) \\ &= \sum_{m\leq n-2} q^{-m} \frac{\bar{\Lambda}(m)}{m} \log(n-m-1) + O(\log n).\end{aligned}$$

To evaluate the last sum, let

$$S_t := \sum_{m\le t} q^{-m}\frac{\bar{\Lambda}(m)}{m}$$

for $t \in \mathbb{N}$ and $S_0 = 0$. Then it equals

$$\begin{aligned}
&\sum_{m\le n-2} (S_m - S_{m-1})\log(n-m-1)\\
&\quad = \sum_{m\le n-3} S_m(\log(n-m-1) - \log(n-m-2)) + O(\log n)\\
&\quad = \sum_{m\le n-3} \log m(\log(n-m-1) - \log(n-m-2)) + O(\log n)\\
&\quad = (\log n)^2 + O(\log n)
\end{aligned}$$

by (3.16), since

$$\begin{aligned}
&\sum_{m\le n-3} \log m(\log(n-m-1) - \log(n-m-2))\\
&\quad = \sum_{m\le n-3} \log\left(1+\frac{1}{m}\right)\log(n-m-2) + O(\log n)\\
&\quad = \sum_{m\le n-3} \frac{1}{m}\left(\log n + \log\left(1-\frac{m+2}{n}\right)\right) + O(\log n)
\end{aligned}$$

and

$$\begin{aligned}
\sum_{m\le \frac{n}{2}} \frac{1}{m}\log\left(1-\frac{m+2}{n}\right) &\ll \log n\\
\sum_{\frac{n}{2}<m\le n-3} \frac{1}{m}\log\left(1-\frac{m+2}{n}\right) &\ll \frac{1}{n}\sum_{\frac{n}{2}<m\le n-3} |\log(n-m-2)-\log n| \ll \log n.
\end{aligned}$$

Hence, the second term on the right–hand side of (3.20) is

$$Aq^n(\log n)^2 + O(q^n\log n).$$

To estimate the last term on the right–hand side of (3.20), we have

$$\sum_{\partial(pp')<n} q^{-\partial(pp')}(n-\partial(pp'))^{-\gamma}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

$$= \sum_{m \le n-1} q^{-m}(n-m)^{-\gamma} \sum_{\partial(pp')=m} 1$$

$$\ll \sum_{m \le n-1} \frac{1}{(n-m)^{\gamma}} \frac{\log m}{m}$$

$$\ll n^{-\gamma+1} + \frac{\log n}{n},$$

since

$$\sum_{\partial(pp')=m} 1 \ll q^m \frac{\log m}{m}$$

and

$$\begin{aligned} \sum_{m \le n-1} \frac{1}{(n-m)^{\gamma}} \frac{\log m}{m} &= \left( \sum_{m \le \frac{n-2}{2}} + \sum_{\frac{n-2}{2} < m \le n-1} \right) \frac{1}{(n-m)^{\gamma}} \frac{\log m}{m} \\ &\ll n^{-\gamma+1} + \frac{\log n}{n}. \end{aligned}$$

Hence the last term on the right–hand side of (3.20) is

$$O\left(q^n \left(n^{-\gamma+1} + n^{-1}\log n\right)\right).$$

This gives

$$\sum_{\partial(pp') \le n} G(n - \partial(pp')) = Aq^n(\log n)^2 + O(q^n \log n)$$

and then

$$\sum_{\partial(a)=n} (\omega(a))^2 = Aq^n(\log n)^2 + O(q^n \log n).$$

We now have

$$\#\left\{a : \partial(a) = n,\ |\omega(a) - \log n| \ge (\log n)^{\frac{1}{2}+\delta}\right\}$$

$$\le (\log n)^{-1-\delta} \sum_{\partial(a)=n} (\omega(a) - \log n)^2$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

$$= (\log n)^{-1-\delta}\Big[\sum_{\partial(a)=n}(\omega(a))^2 - 2\log n\sum_{\partial(a)=n}\omega(a)$$

$$+ (\log n)^2 G(n)\Big]$$

$$= (\log n)^{-1-\delta}\Big[Aq^n(\log n)^2 - 2q^n\log n\,(A\log n + O(1))$$

$$+ (\log n)^2 Aq^n + O(q^n\log n)\Big]$$

$$= O\left(q^n(\log n)^{-\delta}\right). \qquad \square$$

Theorem 3.3.7 gives us some information about the distribution of values of $\omega(a)$ and $\Omega(a)$ about their "mean". For any real-valued function $f$ defined on $\mathcal{G}$, we say that $f$ has **normal** value $F(n)$ for elements of degree $n$ in $\mathcal{G}$ if and only if

$$(1-\varepsilon)F(n) < f(a) < (1+\varepsilon)F(n)$$

holds for "almost all" $a \in \mathcal{G}$ of degree $n$ (i.e., for all but $o(G(n))$ elements $a$ of degree $n$), and for each fixed $\varepsilon > 0$. Theorem 3.3.7 implies that the mean values of $\omega$ and $\Omega$ are essentially also their "normal" values. More accurate information about the distribution of values of $\omega$ and $\Omega$ will be obtained in Chapter 7 by deeper methods.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

## 3.4 Abstract Prime Number Theorems and Zeros of the Generating Function

With the aim of deriving sharper asymptotic information about the numbers $P(n)$, we shall first investigate the relation between abstract prime number theorems and the zeros of the modified zeta (i.e. generating) function

$$Z(y) := \sum_{n=0}^{\infty} G(n)y^n = \prod_{m=1}^{\infty} (1 - y^m)^{-P(m)} \tag{4.1}$$

of $\mathcal{G}$. By the proof of Proposition 1.2.1 earlier, the infinite "Euler" product on the right–hand side converges absolutely and hence the generating function $Z(y)$ has no zeros in the disk $\{|y| < q^{-1}\}$, if $G(n) \ll q^n$. However, for the derivation of abstract prime number theorems in the classical sense, the zero–free region of $Z(y)$ must be extended to include the circle $|y| = q^{-1}$, as the following theorem shows.

(3.4.1) THEOREM. *Suppose that there exist constants $q > 1$ and $\gamma > 1$ such that*

$$\bar{\Lambda}(n) \sim q^n, \quad (\text{“}P.N.T.\text{”}) \tag{4.2}$$

*and*

$$G(n) - qG(n-1) = O(q^n n^{-\gamma}) \tag{4.3}$$

*both hold.* Then $Z(y)$ has no zeros on the circle $|y| = q^{-1}$.

*Remarks.* Condition (3.12) with $\gamma > 1$ implies (4.3) and, conversely, condition (4.3) implies that $G(n) = Aq^n + O(q^n n^{-\gamma+1})$. Thus the "P.N.T." condition (4.2) is equivalent to $P(n) \sim q^n n^{-1}$ by Proposition 3.1.7, if (4.3) holds.

PROOF. To prove Theorem 3.4.1, we need the following inequality:

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

(3.4.2) Lemma. *Let $\gamma$ be a constant satisfying $1 < \gamma < 2$. Then*

$$\sum_{n=1}^{\infty} \frac{x_1^n - x_2^n}{n^\gamma} \ll (x_1 - x_2)^{\gamma - 1}, \quad \textit{for } 0 \le x_1 - x_2 < 1.$$

Proof. Actually

$$\begin{aligned}\sum_{n=1}^{\infty} \frac{x_1^n - x_2^n}{n^\gamma} &= \sum_{n \le (x_1 - x_2)^{-1}} \frac{x_1^n - x_2^n}{n^\gamma} + \sum_{n > (x_1 - x_2)^{-1}} \frac{x_1^n - x_2^n}{n^\gamma} \\ &= \Sigma_1 + \Sigma_2,\end{aligned}$$

say. It is easy to see that

$$\begin{aligned}\Sigma_1 &\le (x_1 - x_2) \sum_{n \le (x_1 - x_2)^{-1}} \frac{1}{n^{\gamma - 1}} \le (x_1 - x_2) \left(1 + \int_1^{(x_1 - x_2)^{-1}} x^{-\gamma + 1} dx\right) \\ &\ll (x_1 - x_2)^{\gamma - 1},\end{aligned}$$

and that

$$\Sigma_2 \le \sum_{n > (x_1 - x_2)^{-1}} n^{-\gamma} \le (x_1 - x_2)^\gamma + \int_{(x_1 - x_2)^{-1}}^{\infty} x^{-\gamma} dx \ll (x_1 - x_2)^{\gamma - 1}. \quad \square$$

Proof of Theorem 3.4.1. Consider the function

$$Z_0(y) := (1 - qy) Z(y) = 1 + \sum_{n=1}^{\infty} \left(G(n) - qG(n-1)\right) y^n,$$

which has a continuous continuation to the circle $|y| = q^{-1}$, by (4.3). It suffices to show that $Z_0(y)$ has no zeros on $|y| = q^{-1}$.

On the one hand, by (1.7), we have

$$\Lambda^{\#}(y) - \frac{qy}{1 - qy} = \sum_{n=1}^{\infty} \left(\bar{\Lambda}(n) - q^n\right) y^n = y \frac{Z_0'(y)}{Z_0(y)}, \quad |y| < q^{-1}.$$

Let $a_n = \bar{\Lambda}(n) - q^n$. Then, by (4.2), $a_n = o(q^n)$. It turns out that

$$\log\left(Z_0(re^{i\theta})\right) = \sum_{n=1}^{\infty} \frac{a_n}{n} r^n e^{in\theta}, \quad 0 \le r < q^{-1},$$

since $Z_0(0) = 1$. Therefore, for any given $\varepsilon > 0$, we have

$$\begin{aligned} |Z_0(re^{i\theta})| &= \exp\left\{Re \sum_{n=1}^{\infty} \frac{a_n q^{-n}}{n} (rq)^n e^{in\theta}\right\} \\ &\ge e^{-c} \exp\left\{-\varepsilon \sum_{n=1}^{\infty} \frac{(rq)^n}{n}\right\} \\ &= e^{-c}(1 - rq)^{\varepsilon}, \end{aligned} \tag{4.4}$$

where $c = c(\varepsilon)$ is a constant since $Re(a_n q^{-n} e^{in\theta}) > -\varepsilon$ for $n \ge n_0$. On the other hand, by (4.3),

$$\begin{aligned} \left|Z_0(r_1 e^{i\theta}) - Z_0(re^{i\theta})\right| &\le \sum_{n=1}^{\infty} |G(n) - qG(n-1)| \left(r_1^n - r^n\right) \\ &\ll \sum_{n=1}^{\infty} \frac{1}{n^{\gamma}} \left((qr_1)^n - (qr)^n\right) \end{aligned}$$

for $0 \le r < r_1 < q^{-1}$. It follows that

$$\left|Z_0(r_1 e^{i\theta}) - Z_0(re^{i\theta})\right| \ll (qr_1 - qr)^{\gamma - 1} \tag{4.5}$$

from Lemma 3.4.2.

Now suppose that Theorem 3.4.1 is false and $Z_0(q^{-1}e^{i\theta}) = 0$. Then, upon letting $r_1 \to q^{-1}$ in (4.5), we would obtain

$$\left|Z_0(re^{i\theta})\right| \ll (1 - qr)^{\gamma - 1}.$$

Taking $\varepsilon = (\gamma - 1)/2$ in (4.4), we would have

$$e^{-c}(1 - qr)^{(\gamma-1)/2} \le K(1 - qr)^{\gamma - 1},$$

or

$$e^{-c}/K \le (1 - qr)^{(\gamma-1)/2};$$

this is certainly absurd for $r$ sufficiently close to $q^{-1}$. □

Conversely, we have the following result which is a "conditional" abstract prime number theorem and an "inverse" of Theorem 3.4.1 in some sense.

(3.4.3) THEOREM. *Suppose that there exists a constant $q > 1$ such that*

$$\sum_{n=1}^{\infty} q^{-2n} n^2 \left|G(n) - qG(n-1)\right|^2 < \infty. \tag{4.6}$$

*If $Z_0(y) = (1 - qy)Z(y)$ is continuous on the closed disk $\{|y| \leq q^{-1}\}$ and has no zeros on the circle $|y| = q^{-1}$, then*

$$\bar{\Lambda}(n) \sim q^n \text{ ("P.N.T.").}$$

PROOF. First note that the condition (4.6) implies

$$G(n) - qG(n-1) = o(q^n n^{-1}).$$

Hence

$$\begin{aligned} G(n) &= (G(n) - qG(n-1)) + q\,(G(n-1) - qG(n-2)) \\ &\quad + \cdots + q^{n-1}\,(G(1) - qG(0)) + q^n \\ &= q^n + q^n \sum_{m=1}^{n} o(m^{-1}) \\ &= o\left(q^n \log n\right). \end{aligned}$$

Then the absolute convergence of $Z(y) = \prod_{m=1}^{\infty}(1 - y^m)^{-P(m)}$ for $|y| < q^{-1}$ follows from a similar argument to the one in the proof of Proposition 1.2.1 since $P(n) \leq G(n)$. We then have

$$\Lambda^{\#}(y) = \sum_{n=1}^{\infty} \bar{\Lambda}(n) y^n = \frac{qy}{1-qy} + y\,\frac{Z_o'(y)}{Z_0(y)}, \quad |y| < q^{-1}.$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Therefore,

$$\bar{\Lambda}(n) = q^n + \frac{1}{2\pi i}\int_{|y|=r} \frac{Z_0'(y)}{Z_0(y)} y^{-n}dy$$

with $0 < r < q^{-1}$. We note that

$$\begin{aligned}&\int_{-\pi}^{\pi} \left|Z_0'(re^{i\theta}) - Z_0'(r_1e^{i\theta})\right|^2 d\theta \\ &= 2\pi \sum_{n=1}^{\infty} n^2 \left(G(n) - qG(n-1)\right)^2 q^{-2n+2} \left((qr)^{n-1} - (qr_1)^{n-1}\right)^2 \\ &\to 0 \quad \text{as } r,\ r_1 \to q^{-1}-,\end{aligned}$$

by (4.6), since $\left((qr)^{n-1} - (qr_1)^{n-1}\right)^2 < 1$. Therefore there exists a function $F(\theta) \in L_2[-\pi,\pi]$ such that $Z_0'(re^{i\theta}) \to F(\theta)$ in $L_2[-\pi,\pi]$ as $r \to q^{-1}-$, by the completeness of the space $L_2[-\pi,\pi]$. It follows that

$$\lim_{r\to q^{-1}-} \frac{1}{2\pi i}\int_{|y|=r} \frac{Z_0'(y)}{Z_0(y)} y^{-n}dy = \frac{q^{n-1}}{2\pi}\int_{-\pi}^{\pi} e^{-(n-1)i\theta}\frac{F(\theta)}{Z_0(q^{-1}e^{i\theta})}\,d\theta$$

since $Z_0(y)$ is continuous in $\{|y| \le q^{-1}\}$ and has no zeros on it. Therefore we obtain

$$\begin{aligned}\bar{\Lambda}(n) &= q^n + \frac{q^{n-1}}{2\pi}\int_{-\pi}^{\pi} e^{-(n-1)i\theta}\frac{F(\theta)}{Z_0(q^{-1}e^{i\theta})}\,d\theta \\ &= q^n + o(q^n),\end{aligned}$$

because the last integral tends to zero as $n \to \infty$, by the Riemann–Lebesgue lemma. □

(3.4.4) COROLLARY. *Suppose there exist constants $q > 1$, $A > 0$ and $\gamma > \frac{3}{2}$, such that*

$$G(n) = Aq^n + O\left(q^n n^{-\gamma}\right).$$

*If $Z_0(y)$ had no zeros on the circle $|y| = q^{-1}$ then $\bar{\Lambda}(n) \sim q^n$.*

*Note.* The condition $\gamma > \frac{3}{2}$ can be replaced by $\gamma > 1$, as shown by Warlimont [1]. We shall not pursue this result here.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

The next theorem is also a "conditional" abstract prime number theorem, but with a remainder term.

(3.4.5) THEOREM. *Suppose that $\mathcal{G}$ satisfies Axiom $\mathcal{A}^{\#}$, i.e. there exist constants $A > 0$, $q > 1$, and $\nu$ with $0 \leq \nu < 1$ such that*

$$G(n) = Aq^n + O(q^{\nu n}). \tag{4.7}$$

*If the generating function $Z(y)$ has no zeros on the circle $|y| = q^{-1}$ then*

$$\bar{\Lambda}(n) = q^n + O(q^{\theta n}) \tag{4.8}$$

*holds for some $\theta$ with $\nu < \theta < 1$.*

*Remark.* In addition to (4.7), Indlekofer [1] makes the assumption that the function $Z_0(y) = (1 - qy)Z(y)$, for $|y| < q^{-1}$ is of *Nevanlinna type.* This leads to still more precise information about the remainder in (4.8).

PROOF. Note that the function $Z_0(y) = (1-qy)Z(y)$ is holomorphic in the disk $\{|y| < q^{-\nu}\}$ by (4.7), and has no zeros in the closed disk $\{|y| \leq q^{-1}\}$. Therefore, by the compactness of the circle $|y| = q^{-1}$, there exists some constant $\theta_1$ with $\nu \leq \theta_1 < 1$ such that $Z_0(y)$ has no zeros in $\{|y| < q^{-\theta_1}\}$. If we shift the integration path in the formula

$$\bar{\Lambda}(n) = \frac{1}{2\pi i}\int_{|y|=r} \frac{Z'(y)}{Z(y)} y^{-n} dy = q^n + \frac{1}{2\pi i}\int_{|y|=r} \frac{Z_0'(y)}{Z_0(y)} y^{-n} dy,$$

with $r < q^{-1}$, to a circle with radius $r = q^{-\theta}$ where $\theta_1 < \theta < 1$, then we arrive at the conclusion. □

## 3.5 Explicit Abstract Prime Number Theorems

### 3.5.1 Versions of Zhang [1]

The results of Section 3.4 show that a key to establishing an abstract prime number theorem in the classical sense is to discover conditions which guarantee that the generating function $Z(y)$ has no zeros on the circle $|y| = q^{-1}$. For this, we first have the following theorem, which is sharp as Example 3.8.1 below will show.

(3.5.1) THEOREM. *If there exist constants $q > 1$ and $A > 0$ such that*

$$\sum_{n=1}^{\infty} \left(G(n) - Aq^n\right)^2 q^{-n} < \infty \tag{5.1}$$

*then $Z(y)$ has no zeros on the circle $|y| = q^{-1}$.*

PROOF. The following proof is a simplication of the one first given by Zhang [1]. To prove Theorem 3.5.1, we first note that, by (5.1),

$$\left(G(n) - Aq^n\right)^2 = o(q^n)$$

and hence

$$G(n) = Aq^n + o\left(q^{\frac{n}{2}}\right).$$

Therefore, essentially as in the proof of Proposition 1.2.1, one sees that $Z(y)$ has an analytic continuation in the disk $\left\{|y| < q^{-\frac{1}{2}}\right\}$ as a meromorphic function, with the only singularity being a pole of order one at $y = q^{-1}$. We divide the further proof of Theorem 3.5.1 into several lemmas.

(3.5.2) LEMMA. *Assume Axiom $\mathcal{A}^{\#}$, i.e. suppose there exist constants $A > 0$, $q > 1$, and $\nu$ with $0 \leq \nu < 1$, such that*

$$G(n) = Aq^n + O(q^{\nu n}).$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

*Then $Z(y)$ has no zeros on the circle $|y| = q^{-1}$, except perhaps at the point $y = -q^{-1}$ where it has at most a simple zero.*

PROOF. Consider the "associated zeta function" $\zeta(s) := Z(q^{-s})$ with $\mathcal{R}e\, s = \sigma > \frac{1}{2}$, (*not* to be confused with the *Riemann* zeta function). Then

$$\zeta(\sigma + it) = \prod_{m=1}^{\infty} \left(1 - q^{-m(\sigma+it)}\right)^{-P(m)}$$

for $\sigma > 1$, and we have

$$\zeta(\sigma) = Z(q^{-\sigma}) = \sum_{n=0}^{\infty} G(n) q^{-n\sigma} = \frac{A/\log q}{\sigma - 1}(1 + O(\sigma - 1))$$

as $\sigma \to 1+$. Since

$$\begin{aligned}
&(\zeta(\sigma))^3 \left|\zeta(\sigma + it)\right|^4 \left|\zeta(\sigma + 2it)\right| \\
&= \exp\left\{ \sum_{m=1}^{\infty} P(m) \sum_{k=1}^{\infty} \frac{1}{k} q^{-mk\sigma} \Big(3 + 4\cos(tkm \log q) \\
&\quad + \cos(2tkm \log q)\Big) \right\} \\
&\geq 1 \text{ for } \sigma > 1,
\end{aligned}$$

in view of $3 + 4\cos\theta + \cos 2\theta = 2(\cos\theta + 1)^2 \geq 0$, $\zeta(\sigma + it)$ has no zeros on the line $\sigma = 1$ except possibly at those points with $t = m\pi/\log q$, $m = \pm 1, \pm 3, \ldots$, where it has a zero of order at most one. Therefore $Z(y)$ has no zeros on the circle $|y| = q^{-1}$, except possibly at the point $y = -q^{-1}$ where it has at most a simple zero. □

(3.5.3) LEMMA. *Assume (5.1), and suppose that $Z(y)$ has a zero at $y = -q^{-1}$. Let*

$$Z(y)Z(-y) = 1 + \sum_{n=1}^{\infty} H(n) y^n.$$

*Then*

$$H(n) = o\left(q^{\frac{n}{2}}\right). \tag{5.2}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

PROOF. We first show that

$$\lim_{r,r_1\to q^{-\frac{1}{2}}-}\int_{-\pi}^{\pi}\left|Z(re^{i\theta})-Z(r_1e^{i\theta})\right|^2 d\theta = 0. \tag{5.3}$$

Actually, we have

$$Z(y) = g(y) + f(y)$$

where

$$g(y) = \frac{Aqy}{1-qy}, \quad f(y) = 1 + \sum_{n=1}^{\infty}\left(G(n) - Aq^n\right)y^n.$$

The function $f(y)$ is holomorphic in the disk $\{|y| < q^{-\frac{1}{2}}\}$ by (5.1) and we have

$$\begin{aligned}\int_{-\pi}^{\pi}&\left|f(re^{i\theta})-f(r_1e^{i\theta})\right|^2 d\theta\\ &= 2\pi\sum_{n=1}^{\infty}\left(G(n)-Aq^n\right)^2 q^{-n}\left(\left(q^{\frac{1}{2}}r\right)^n-\left(q^{\frac{1}{2}}r_1\right)^n\right)^2\end{aligned}$$

for $r < q^{-\frac{1}{2}}$, $r_1 < q^{-\frac{1}{2}}$. We note that $\left(\left(q^{\frac{1}{2}}r\right)^n-\left(q^{\frac{1}{2}}r_1\right)^n\right)^2 < 1$. Therefore, by (5.1),

$$\lim_{r,r_1\to q^{-\frac{1}{2}}-}\int_{-\pi}^{\pi}\left|f(re^{i\theta})-f(r_1e^{i\theta})\right|^2 d\theta = 0.$$

Also, note that $g(y)$ is uniformly continuous on the annulus $\left\{q^{-\frac{2}{3}} \le |y| \le q^{-\frac{1}{2}}\right\}$. Therefore (5.3) follows from the inequality

$$\begin{aligned}&\left|Z(re^{i\theta})-Z(r_1e^{i\theta})\right|^2\\ &\quad\le 2\left(\left|g(re^{i\theta})-g(r_1e^{i\theta})\right|^2+\left|f(re^{i\theta})-f(r_1e^{i\theta})\right|^2\right).\end{aligned}$$

Now consider $Z(y)Z(-y)$. By the hypothesis that $Z(y)$ has a zero at $y = -q^{-1}$, $Z(y)Z(-y)$ has no poles at $y = q^{-1}$ and $y = -q^{-1}$. Therefore, it

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

is holomorphic in the disk $\left\{|y| < q^{-\frac{1}{2}}\right\}$. We have

$$\begin{aligned} H(n) &= \frac{1}{2\pi i}\int_{|y|=r} \frac{Z(y)Z(-y)}{y^{n+1}}\,dy \\ &= \frac{1}{2\pi r^n}\int_{-\pi}^{\pi} e^{in\theta} Z(re^{i\theta})Z(-re^{i\theta})d\theta. \end{aligned} \qquad (5.4)$$

By (5.3), there exists a function $F(\theta) \in L_1[-\pi,\pi]$ such that

$$\lim_{r\to q^{-\frac{1}{2}}-} \int_{-\pi}^{\pi} \left|Z(re^{i\theta})Z(-re^{i\theta}) - F(\theta)\right| d\theta = 0.$$

Therefore, if we take the limit as $r \to q^{-\frac{1}{2}}-$ on the right–hand side of (5.4), then we obtain

$$H(n) = \frac{q^{\frac{n}{2}}}{2\pi}\int_{-\pi}^{\pi} e^{in\theta}F(\theta)d\theta.$$

It follows that $H(n) = o\left(q^{\frac{n}{2}}\right)$, since the last integral tends to zero as $n \to \infty$ by the Riemann–Lebesgue lemma. □

PROOF OF THEOREM 3.5.1 Write

$$Z(y)Z(-y) = \prod_{\substack{m=1\\ m \text{ even}}}^{\infty} \left(\frac{1+y^m}{1-y^m}\right)^{P(m)} Z(y^2)$$

and

$$Z(y^2) = \sum_{n=0}^{\infty} G_1(n)y^n,$$

$$\prod_{\substack{m=1\\ m \text{ even}}}^{\infty} \left(\frac{1+y^m}{1-y^m}\right)^{P(m)} = \sum_{n=0}^{\infty} G_2(n)y^n.$$

Then

$$G_1(n) = \begin{cases} G\left(\frac{n}{2}\right), & \text{if } n \text{ is even;} \\ 0, & \text{if } n \text{ is odd.} \end{cases}$$

Also, since

$$\frac{1+y^m}{1-y^m} = (1+y^m)\sum_{k=0}^{\infty} y^{km}$$

and the $P(m)$ are non-negative integers, the $G_2(n)$ are all non-negative integers. Therefore

$$1 + \sum_{n=1}^{\infty} H(n)y^n = \left(\sum_{n=0}^{\infty} G_1(n)y^n\right)\left(\sum_{n=0}^{\infty} G_2(n)y^n\right),$$

and

$$\begin{aligned} H(n) &= G_1(n) + G_2(1)G_1(n-1) + \cdots + G_1(n-1)G_1(1) + G_2(n) \\ &\geq G_1(n). \end{aligned}$$

Suppose that Theorem 3.5.1 is not true, and that $Z(y)$ has a zero at $y = -q^{-1}$. Then we would have

$$\liminf_{n\to\infty} q^{-n}H(2n) \geq \lim_{n\to\infty} q^n G(n) = A > 0;$$

this contradicts (5.2). □

Theorem 3.5.1 has the following direct corollary which is convenient to apply.

(3.5.4) COROLLARY. *If there exist constants $q > 1$, $A > 0$, and $\gamma > \frac{1}{2}$, such that*

$$G(n) = Aq^n + O\left(q^{\frac{n}{2}} n^{-\gamma}\right)$$

*then $Z(y)$ has no zeros on the circle $|y| = q^{-1}$.*

This corollary combined with Example 3.8.1 below shows that Theorem 3.5.1 is in some sense "sharp".

Furthermore, by combining Corollary 3.5.4 and Theorem 3.4.5, we obtain the following abstract prime number theorem.

(3.5.5) THEOREM. *Suppose that there exist constants $q > 1$, $A > 0$, and $\nu$ with $0 \leq \nu < \frac{1}{2}$ such that*

$$G(n) = Aq^n + O(q^{\nu n}), \quad n = 1, 2, \ldots,$$

*or that (for $\nu = \frac{1}{2}$) there exists also a constant $\gamma > \frac{1}{2}$ such that*

$$G(n) = Aq^n + O\left(q^{\frac{n}{2}}n^{-\gamma}\right), \quad n = 1, 2, \ldots .$$

*Then*

$$\bar{\Lambda}(n) = q^n + O(q^{\theta n}) \tag{5.5}$$

*holds for some $\theta$ with $\nu \le \theta < 1$.*

*Remark.* Theorem 3.5.5 gives rise to the problem initiated by S.D. Cohen [1] to describe more precisely in terms of $\nu$ the quantity $\theta$ in the remainder of (5.5). Example 3.8.6 below will show that there is not too much we can say about $\theta$ in terms of $\nu$.

### 3.5.2 Versions of Indlekofer–Manstavicius–Warlimont [1]

Now consider some theorems given by (or equivalent to ones given by) Indlekofer, Manstavicius and Warlimont [1].

(3.5.6) THEOREM. *Assume $P(n) \ll q^n$, $n = 1, 2, \ldots$, for some $q > 1$. Suppose that $Z(y)$ can be analytically continued in the disk $\left\{|y| < q^{-\frac{1}{2}}\right\}$ to a meromorphic function with only singularity being a simple pole at $y = q^{-1}$. If*

$$\liminf_{x \to q^{-\frac{1}{2}}-} \left(1 - q^{\frac{1}{2}}x\right) Z(x)Z(-x) \le 0 \tag{5.6}$$

*then $Z(y)$ has no zeros on the circle $|y| = q^{-1}$.*

*Remark 1.* This theorem implies that, if

$$\lim_{x \to q^{-\frac{1}{2}}-} \left(1 - q^{\frac{1}{2}}x\right) Z(x)Z(-x) = 0, \tag{5.7}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

then $Z(y)$ has no zeros on the circle $|y| = q^{-1}$. This is a weaker and non-equivalent conclusion.

*Remark 2.* One can deduce Theorem 3.5.1 from Theorem 3.5.6. Actually, (5.1) implies the conditions of Theorem 3.5.6 as well as (5.2) by Lemma 3.5.3. From (5.2), we have

$$Z(x)Z(-x) \leq 1 + \sum_{n=1}^{n_0} H(n)x^n + \sum_{n=n_0+1}^{\infty} \varepsilon q^{\frac{n}{2}} x^n$$

for $0 \leq x < q^{-\frac{1}{2}}$. Hence

$$\left(1 - q^{\frac{1}{2}}x\right) Z(x)Z(-x) \leq \left(1 - q^{\frac{1}{2}}x\right)\left(1 + \sum_{n=1}^{n_0} H(n)x^n\right) + \varepsilon q^{\frac{n_0+1}{2}} x^{n_0+1},$$

and then

$$\limsup_{x \to q^{-\frac{1}{2}}-} \left(1 - q^{\frac{1}{2}}x\right) Z(x)Z(-x) \leq \varepsilon$$

for each $\varepsilon > 0$. Thus (5.6) follows.

Theorem 3.5.6 is an equivalent form to:

(3.5.7) THEOREM. *Assume the conditions of Theorem 3.5.6. If $Z(-q^{-1}) = 0$, then*

$$\left(1 - q^{\frac{1}{2}}x\right)^{-1} \ll Z(x)Z(-x) \tag{5.8}$$

*for real $x \to q^{-\frac{1}{2}}-$.*

PROOF. Actually, (5.8) holds if and only if

$$\liminf_{x \to q^{-\frac{1}{2}}-} \left(1 - q^{\frac{1}{2}}x\right) Z(x)Z(-x) \geq c \tag{5.9}$$

for some $c > 0$. If $Z(-q^{-1}) = 0$, then Theorem 3.5.6 implies (5.9), and Theorem 3.5.7 follows. Conversely, if (5.6) holds, then (5.9) does not, and,

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

by Theorem 3.5.7, $Z(-q^{-1}) \neq 0$. Thus $Z(y)$ has no zeros on the circle $|y| = q^{-1}$, by Lemma 3.5.2. Then Theorem 3.5.6 follows. □

PROOF OF THEOREM 3.5.7 As in the proof of Theorem 3.5.1, we have

$$Z(y)Z(-y) = g(y)Z(y^2), \quad |y| < q^{-1},$$

where

$$g(y) := \prod_{\substack{n=1 \\ n \text{ even}}}^{\infty} \left(\frac{1+y^n}{1-y^n}\right)^{P(n)}.$$

Note that $g$ is holomorphic for $|y| < q^{-1}$ and that $g(0) = 1$. Let

$$g(y) = 1 + \sum_{n=1}^{\infty} c_n y^n, \quad |y| < q^{-1}. \tag{5.10}$$

Then $c_n \geq 0$. We note that the functions $Z(y^2)$ and $\frac{1-qy}{1+qy}Z(y)$ are holomorphic for $|y| < q^{-\frac{1}{2}}$ and that $Z(y^2) \neq 0$ there. Hence

$$g(y) = \frac{1}{Z(y^2)}\left(\frac{1-qy}{1+qy}Z(y)\right)\left(\frac{1+qy}{1-qy}Z(-y)\right)$$

is holomorphic there too. Therefore the power series expansion (5.10) holds for $|y| < q^{-\frac{1}{2}}$ too. We then obtain

$$g(x) \geq 1$$

for $0 \leq x < q^{-\frac{1}{2}}$. It follows that

$$Z(x)Z(-x) \geq Z(x^2)$$

for $0 \leq x < q^{-\frac{1}{2}}$. Since $Z(y^2)$ has a simple pole at $y = q^{-\frac{1}{2}}$, and $Z(x^2) > 0$ for $0 \leq x < q^{-\frac{1}{2}}$, we see that

$$\left(1 - q^{\frac{1}{2}}x\right)^{-1} \ll Z(x^2)$$

for $0 \leq x < q^{-\frac{1}{2}}$, and (5.8) follows. □

(3.5.8) Example. As in Theorem 2.1.1 earlier, consider the generating function $Z_{\mathcal{F}_q}(y)$ of the category $\mathcal{F}_q$. Then, as before,

$$Z_{\mathcal{F}_q}(y) = \prod_{r=1}^{\infty}(1-qy^r)^{-1}.$$

Hence, for $0 \leq x < q^{-\frac{1}{2}}$,

$$\left(1-q^{\frac{1}{2}}x\right) Z_{\mathcal{F}_q}(x)Z_{\mathcal{F}_q}(-x)$$

$$= \left(1-q^{\frac{1}{2}}x\right)\prod_{r \text{ odd}}\left(1-q^2x^{2r}\right)^{-1}\prod_{s=1}^{\infty}\left(1-qx^{2s}\right)^{-2}$$

$$= \left(1-q^{\frac{1}{2}}x\right)^{-1}\left(1+q^{\frac{1}{2}}x\right)^{-2}\prod_{r \text{ odd}}\left(1-q^2x^{2r}\right)^{-1}\prod_{s=2}^{\infty}\left(1-qx^{2s}\right)^{-2}.$$

As $x \to q^{-\frac{1}{2}}-$, $\left(1-q^{\frac{1}{2}}x\right)^{-1} \to +\infty$ and

$$\lim_{x\to q^{-\frac{1}{2}}-}\prod_{r \text{ odd}}\left(1-q^2x^{2r}\right)^{-1} = (1-q)^{-1}\prod_{\substack{r \text{ odd}\\ r\geq 3}}\left(1-q^{2-r}\right)^{-1} < 0,$$

$$\lim_{x\to q^{-\frac{1}{2}}-}\prod_{s=2}^{\infty}\left(1-qx^{2s}\right)^{-2} = \prod_{s=2}^{\infty}\left(1-q^{1-s}\right)^{-1} > 0.$$

Hence, we have

$$\lim_{x\to q^{-\frac{1}{2}}-}\left(1-q^{\frac{1}{2}}x\right) Z_{\mathcal{F}_q}(x)Z_{\mathcal{F}_q}(-x) = -\infty.$$

By Theorem 3.5.6, $Z_{\mathcal{F}_q}(y)$ has no zeros on the circle $|y| = q^{-1}$. Thus the total number $P_{\mathcal{F}}(n)$ of non-isomorphic *indecomposable* modules of cardinal $q^n$ satisfies

$$P_{\mathcal{F}}(n) = \frac{q^n}{n} + O(q^{\theta n})$$

as $n \to \infty$, where $\frac{1}{2} \leq \theta < 1$, which is a weaker form of Proposition 3.1.1 above.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

## 3.6 A Tauberian Theorem of Bombieri

The proofs of the abstract prime number theorms given so far are analytic. Elementary proofs can be constructed on the basis of the following tauberian theorem (cf. Zhang [4]), which is a refinement of one of Bombieri [2].

(3.6.1) THEOREM. *Suppose that* $a_m \geq 0$, $m = 1, 2, \ldots,$ *and that*

$$ma_m + \sum_{i=1}^{m-1} a_i a_{m-i} = 2m + O(1), \tag{6.1}$$

*and*

$$\sum_{i=1}^{m} a_{2i} = m + O(1), \tag{6.2}$$

*as* $m \to \infty$. *Then*

$$a_m = 1 + O\left(\frac{1}{m}\right) \text{ as } m \to \infty.$$

*Remark 1.* Let $a_m = 1$ if $m$ is not a square of an integer, and $a_{n^2} = 1 + \frac{1}{n^2}$ for $n \geq 1$. Then plainly the conditions of Theorem 3.6.1 are satisfied. This example shows that $a_m = 1 + O\left(\frac{1}{m}\right)$ is sharp.

*Remark 2.* The condition (6.2) cannot be replaced by the condition

$$\sum_{i=1}^{m} a_i = m + O(1). \tag{6.3}$$

A counter–example is $a_n = 2$ if $n$ is odd, and $a_n = 0$ if $n$ is even. Then the $a_n$ satisfy (6.1) and (6.3), but not (6.2). A tauberian theorem of Erdős [1] shows that (6.1) implies (6.3). Therefore, the condition (6.1), together with the non–negativity of $a_n$ is not alone sufficient to imply $a_m = 1 + o(1)$. To

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

guarantee the convergence of $a_m$ as $m \to \infty$, some other condition beyond (6.1) (and its implication (6.3)) is needed. This reveals another important divergence of the theory of additive arithmetical semigroups exposed in this monograph from classical number theory. As is well-known, in classical number theory (see, e.g. Erdős [1]), the Selberg formula is alone sufficient in order to deduce the prime number theorem for $\mathbb{N}$. However, for additive arithmetical semigroups, the abstract Selberg–Bombieri formula (see (7.2) of Section 3.7) is not sufficient by itself.

*Remark 3.* We shall give a proof of Theorem 3.6.1 with the supplemental condition (6.3). This is merely an equivalent form of Theorem 3.6.1, because, as we mentioned in Remark 2, (6.3) is actually a consequence of (6.1). With the supplemental condition (6.3), our proof of Theorem 3.6.1 is self-contained and shorter, because we have no need to appeal to the proof of Erdős's tauberian theorem. In point of view of being self-contained,Theorem 3.6.1 with supplemental (6.3) will be sufficient to construct elementary proofs of an abstract prime number theorem. Actually, in our elementary proofs, which we shall introduce in the next section, the condition (6.3) is merely the Mertens-type asymptotic estimate (3.2) which was proved in Theorem 3.3.1.

Let $a_m = 1 + r_m$. From (6.1), (6.2), and (6.3), we have

$$mr_m + \sum_{k=1}^{m-1} r_k r_{m-k} = O(1), \tag{6.4}$$

$$\sum_{k=1}^{m} r_k = O(1), \tag{6.5}$$

and

$$\sum_{k=1}^{m} r_{2k} = O(1). \tag{6.6}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Moreover, since $a_m \geq 0$, from (6.1),

$$ma_m \leq 2m + O(1)$$

and then

$$0 \leq 1 + r_m = a_m \leq 2 + O\left(\frac{1}{m}\right).$$

Hence

$$-1 \leq r_m \leq 1 + O\left(\frac{1}{m}\right).$$

Thus we have

$$|r_m| \leq 1 + O\left(\frac{1}{m}\right). \tag{6.7}$$

It suffices to show that $r_m = O\left(\frac{1}{m}\right)$.

To this end, we first prove the following lemma, which is a strengthened form of the lemma given in Bombieri's paper. The proof follows his general idea.

(3.6.2) LEMMA. *We have*

$$\limsup_{m\to\infty} |r_m + r_{m+1}| \leq 1, \quad \limsup_{m\to\infty} |r_m - r_{m+1}| \leq 1. \tag{6.8}$$

*Remark.* This lemma shows that $r_m$ has a kind of slow oscillation, which is essential for proving Theorem 3.6.1.

PROOF. From (6.4) and (6.7), we have

$$m\,|r_m \pm r_{m+1}| \leq \sum_{k=1}^{m-1} |r_k \pm r_{k+1}| + O(\log m). \tag{6.9}$$

To prove the first part of (6.8), suppose on the contrary that

$$\limsup_{m\to\infty} |r_m + r_{m+1}| = \ell > 1.$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Then, for any given $\varepsilon$ positive and sufficiently small, the set

$$M_\varepsilon := \{m \in \mathbb{N} : |r_m + r_{m+1}| > \ell - \varepsilon > 1\}$$

contains infinitely many $m$. For each $m \in M_\varepsilon$, let the set

$$I = I(m, \varepsilon) := \left\{k \in \mathbb{N} : \ k \leq m, \ |r_k + r_{k+1}| \leq \ell - \sqrt{\varepsilon}\right\}.$$

Then, from (6.9), for $m \in M_\varepsilon$, we have

$$m(\ell - \varepsilon) \leq \left(\ell - \sqrt{\varepsilon}\right)|I| + (\ell + \varepsilon)(m - |I|) + O_\varepsilon(\log m),$$

where $|I|$ is the number of $k$'s in $I$. It follows that

$$|I| \leq 2\sqrt{\varepsilon} m + O_\varepsilon(\log m). \tag{6.10}$$

Therefore, if we choose $\varepsilon$ positive and sufficiently small then for $m$ in $M_\varepsilon$ sufficiently large there is an interval $[a, b]$ with integral end points $a$ and $b$ such that

$$\frac{m}{2} \leq a < b \leq m, \quad b - a > \frac{1}{10\sqrt{\varepsilon}}, \tag{6.11}$$

and such that

$$|r_k + r_{k+1}| > \ell - \sqrt{\varepsilon} > 1 \text{ for all } k \in [a, b]. \tag{6.12}$$

Actually, if such an interval $[a, b]$ did not exist, then for every $n$ between $\frac{m}{2}$ and $m$ there would be some $k \in I$ such that $-\frac{1}{10\sqrt{\varepsilon}} \leq n - k \leq \frac{1}{10\sqrt{\varepsilon}}$, and hence the union of the intervals $I_k = \left[k - \frac{1}{9\sqrt{\varepsilon}}, \ k + \frac{1}{9\sqrt{\varepsilon}}\right]$ with $k \in I$ would cover the interval $\left[\frac{m}{2}, m\right]$. However, the total length of intervals $I_k$ is, by (6.10), at most

$$\begin{aligned} |I|\frac{2}{9\sqrt{\varepsilon}} &\leq \frac{2}{9\sqrt{\varepsilon}}\left(2\sqrt{\varepsilon}m + O_\varepsilon(\log m)\right) \\ &= \frac{4}{9}m + \frac{2}{9}O_\varepsilon(\log m) < \frac{m}{2} - 1 - \frac{2}{\sqrt{\varepsilon}} \\ &\leq \left|\left[\frac{m}{2} + \frac{1}{\sqrt{\varepsilon}}, m - \frac{1}{\sqrt{\varepsilon}}\right]\right| \end{aligned}$$

for $m$ sufficiently large, where the two $O_\varepsilon$–constants may be different.

Since $|r_k| \leq 1 + O\left(\frac{1}{k}\right)$, (6.12) shows that $r_k$ and $r_{k+1}$ have the same sign for all $k \in [a, b]$. It follows that

$$\begin{aligned}\left|\sum_{k \in [a,b]} r_k\right| &= \left|\frac{1}{2}\sum_{k \in [a,b-1]} (r_k + r_{k+1}) + \frac{r_a}{2} + \frac{r_b}{2}\right| \\ &\geq \frac{1}{2}\sum_{k \in [a,b-1]} |r_k + r_{k+1}| > \frac{1}{2}(\ell - \sqrt{\varepsilon})(b-a) \\ &> \frac{1}{20\sqrt{\varepsilon}}.\end{aligned}$$

However, from (6.5),

$$\frac{1}{20\sqrt{\varepsilon}} < \left|\sum_{k \in [a,b]} r_k\right| \leq \left|\sum_{k=1}^{b} r_k\right| + \left|\sum_{k=1}^{a-1} r_k\right| = O(1),$$

which is certainly absurd if $\varepsilon$ is small enough. This completes the proof of the first part of (6.8).

Similarly, to prove the second inequality of (6.8), suppose on the contrary that $\limsup_{m\to\infty} |r_m - r_{m+1}| = \ell > 1$. A similar argument shows that there is an interval $[c, d]$ with integral end points $c$ and $d$ such that

$$\frac{m}{2} \leq c < d \leq m, \quad d - c > \frac{1}{10\sqrt{\varepsilon}},$$

and such that

$$|r_k - r_{k+1}| > \ell - \sqrt{\varepsilon} > 1 \text{ for all } k \in [c, d]. \tag{6.13}$$

Since $|r_k| \leq 1 + O\left(\frac{1}{k}\right)$, (6.13) shows that $r_k$ and $r_{k+1}$ have the opposite sign for all $k \in [c, d]$. Then the numbers $r_{2k}$ have the same sign, and the numbers $r_{2k-1} - r_{2k}$ have the same sign, for all $2k \in [c, d]$. It follows, from

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

(6.13) and (6.5), that

$$\begin{aligned}\left|\sum_{2k\in[c,d]} r_{2k}\right| &= \left|\frac{1}{2}\sum_{2k\in[c,d]}(r_{2k-1}+r_{2k}) - \frac{1}{2}\sum_{2k\in[c,d]}(r_{2k-1}-r_{2k})\right| \\ &\geq \frac{1}{2}\sum_{2k\in[c,d]}|r_{2k-1}-r_{2k}| + O(1) \\ &> \frac{\ell-\sqrt{\varepsilon}}{2}\left(\frac{d-c}{2}-2\right)+O(1) \\ &> \frac{1}{40\sqrt{\varepsilon}} - 1 + O(1), \qquad (6.14)\end{aligned}$$

since

$$\sum_{2k\in[c,d]}(r_{2k-1}+r_{2k}) = \sum_{k_1<k\leq k_2} r_k = O(1).$$

Now, (6.14) contradicts (6.6) if $\varepsilon$ is small enough. This proves the second part of (6.8). □

PROOF OF THEOREM 3.6.1. Let $A = \limsup_{m\to\infty}|r_m|$. We first show $A = 0$. From (6.4) and (6.7), $0 \leq A \leq 1$ and $A \leq A^2$. Hence, either $A = 0$ or $A = 1$. If $A = 0$ there is nothing to do. Therefore, we may assume $A = 1$. By (6.4) and (6.7), we have

$$m|r_m| \leq \sum_{k=1}^{m-1}|r_k| + O(\log m).$$

Since $A = 1$, for $\varepsilon$ positive and sufficiently small, there exist infinitely many $m$ such that $|r_m| > 1-\varepsilon$. If we argue as in the proof of Lemma 3.6.2, then for each $m$ sufficiently large there is an interval $[e, f]$ with integral end points $e$ and $f$ such that

$$\frac{m}{2} \leq e < f \leq m, \quad f - e > \frac{1}{10\sqrt{\varepsilon}},$$

and such that

$$|r_k| > 1-\sqrt{\varepsilon} > \frac{2}{3} \text{ for all } k \in [e, f].$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

This inequality contradicts (6.8). Actually, for $k$, $k+1 \in [e,f]$, if $r_k$ and $r_{k+1}$ have the same sign then $|r_k + r_{k+1}| > \frac{4}{3}$ and if $r_k$ and $r_{k+1}$ have the opposite sign then $|r_k - r_{k+1}| > \frac{4}{3}$. Hence, at least one of the limits in (6.8) would exceed 1. This proves $\lim_{m\to\infty} |r_m| = 0$.

It remains to show $r_m = O\left(\frac{1}{m}\right)$. From (6.4), there exists a constant $K$ such that

$$\left| m r_m + \sum_{k=1}^{m-1} r_k r_{m-k} \right| \le K \tag{6.15}$$

holds for $m = 1, 2, \ldots$. We fix a positive integer $m_0$ sufficiently large so that, for $m \ge m_0$,

$$\frac{1}{m}\sum_{k=1}^{m} |r_k| < \frac{1}{4}, \quad |r_m| < \frac{1}{4}. \tag{6.16}$$

We shall show that for every positive integer $k$ if $m \ge 2^k m_0$ then

$$|r_m| \le \left(\frac{1}{4}\right)^{k+1} + \frac{K}{m}\left(1 + \eta + \eta^2 + \cdots + \eta^{k-1}\right) \tag{6.17}$$

where

$$\eta = \frac{1}{4} + \frac{3}{4}\log 2. \tag{6.18}$$

This leads to the conclusion of the theorem immediately. In fact, for any $m \ge 2m_0$, if we take $k$ satisfying $2^{k+1}m_0 > m \ge 2^k m_0$, from (6.17), we shall have

$$\begin{aligned} |r_m| &\le 2^{-2k-2} + \frac{K}{1-\eta}\frac{1}{m} \\ &\le \left(\frac{m_0}{m}\right)^2 + \frac{K}{1-\eta}\frac{1}{m} \le \left(m_0 + \frac{K}{1-\eta}\right)\frac{1}{m}. \end{aligned}$$

To prove (6.17), we first note that, for $k = 1$, (6.17) is certainly true. Actually, we have, from (6.15) and (6.16),

$$|r_m| \le \frac{1}{m}\left\{ 2\sum_{s=1}^{[m/2]} |r_s|\,|r_{m-s}| + K \right\}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

$$\leq \frac{1}{m}\left\{\frac{1}{2}\sum_{s=1}^{[m/2]}|r_s|+K\right\}\leq\left(\frac{1}{4}\right)^2+\frac{K}{m}.$$

Therefore, we assume (6.17) for $1 \leq k \leq \ell$ and consider $m \geq 2^{\ell+1}m_0$. We write $\eta_k = 1+\eta+\eta^2+\cdots+\eta^{k-1}$. Then, by the induction hypothesis,

$$\begin{aligned}
|r_m| &\leq \frac{1}{m}\left\{2\sum_{s=1}^{[m/2]}|r_s|\,|r_{m-s}|+K\right\}\\
&\leq \frac{1}{m}\left\{2\sum_{s=1}^{[m/2]}|r_s|\left(\left(\frac{1}{4}\right)^{\ell+1}+\frac{K}{m-s}\eta_\ell\right)+K\right\}\\
&= \frac{2}{m}\left(\frac{1}{4}\right)^{\ell+1}\sum_{s=1}^{[m/2]}|r_s|+\frac{2K\eta_\ell}{m}\sum_{s=1}^{[m/2]}|r_s|\frac{1}{m-s}+\frac{K}{m} \qquad (6.19)
\end{aligned}$$

since, for $s \leq \left[\frac{m}{2}\right]$, $m-s \geq \frac{m}{2} \geq 2^\ell m_0$. We shall estimate the last two sums in (6.19) separately.

First, by (6.16),

$$\begin{aligned}
\sum_{s=1}^{[m/2]}|r_s|\frac{1}{m-s} &= \sum_{s=1}^{[2^{-\ell-1}m]}|r_s|\frac{1}{m-s}+\sum_{s=[2^{-\ell-1}m]+1}^{[m/2]}|r_s|\frac{1}{m-s}\\
&\leq \frac{1}{4}\left(\frac{1}{m-2^{-\ell-1}m}2^{-\ell-1}m+\sum_{s=[2^{-\ell-1}m]+1}^{[m/2]}\frac{1}{m-s}\right)\\
&\leq \frac{1}{4}\left(\frac{1}{3}+\log 2\right)=\frac{1}{3}\eta
\end{aligned}$$

since

$$\sum_{s=[2^{-\ell-1}m]+1}^{[m/2]}\frac{1}{m-s}=\sum_{k=m-[m/2]}^{m-[2^{-\ell-1}m]-1}\frac{1}{k}\leq\int_{\frac{m}{2}-1}^{m-2}\frac{dt}{t}=\log 2.$$

Hence

$$\frac{2K\eta_\ell}{m}\sum_{s=1}^{[m/2]}|r_s|\frac{1}{m-s}\leq\frac{2}{3}\frac{K}{m}\eta_\ell\eta. \qquad (6.20)$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Secondly, by (6.16) and (6.17) with $1 \leq k \leq \ell$,

$$
\begin{aligned}
\sum_{s=1}^{[m/2]} |r_s| &= \sum_{s=1}^{[2^{-\ell}m]} |r_s| + \sum_{s=[2^{-\ell}m]+1}^{[2^{-\ell+1}m]} |r_s| + \cdots + \sum_{s=[\frac{m}{4}]+1}^{[m/2]} |r_s| \\
&\leq [2^{-\ell}m]\frac{1}{4} + \sum_{s=[2^{-\ell}m]+1}^{[2^{-\ell+1}m]} \left(\left(\frac{1}{4}\right)^2 + \frac{K}{s}\eta_1\right) \\
&\quad + \sum_{s=[2^{-\ell+1}m]+1}^{[2^{-\ell+2}m]} \left(\left(\frac{1}{4}\right)^3 + \frac{K}{s}\eta_2\right) + \cdots \\
&\quad + \sum_{s=[\frac{m}{4}]+1}^{[m/2]} \left(\left(\frac{1}{4}\right)^\ell + \frac{K}{s}\eta_{\ell-1}\right) \\
&\leq \frac{1}{4}\Bigg\{[2^{-\ell}m] + \left([2^{-\ell+1}m] - [2^{-\ell}m]\right)\frac{1}{4} \\
&\quad + \left([2^{-\ell+2}m] - [2^{-\ell+1}m]\right)\left(\frac{1}{4}\right)^2 + \cdots \\
&\quad + \left(\left[\frac{m}{2}\right] - \left[\frac{m}{4}\right]\right)\left(\frac{1}{4}\right)^{\ell-1}\Bigg\} \\
&\quad + K\eta_{\ell-1} \sum_{s=[s^{-\ell}m]+1}^{[m/2]} \frac{1}{s} \\
&= \frac{1}{4}\Sigma_1 + K\eta_{\ell-1} \sum_{s=[2^{-\ell}m]+1}^{[m/2]} \frac{1}{s}, \qquad (6.21)
\end{aligned}
$$

say. Therefore, if $\ell = 1$, we have $\sum_{s=1}^{[m/2]} |r_s| \leq m2^{-\ell}/4$. If $\ell \geq 2$, we have

$$
\Sigma_1 = \frac{3}{4}[2^{-\ell}m] + \frac{3}{4}\frac{1}{4}[2^{-\ell+1}m]
$$

$$\begin{aligned}
&+\frac{3}{4}\left(\frac{1}{4}\right)^{2}[2^{-\ell+2}m]+\cdots+\frac{3}{4}\left(\frac{1}{4}\right)^{\ell-2}\left[\frac{m}{4}\right]\\
&+\left(\frac{1}{4}\right)^{\ell-1}\left[\frac{m}{2}\right]\\
\leq\ &\frac{3}{4}2^{-\ell}m\left(1+\frac{1}{2}+\frac{1}{2^2}+\cdots+\frac{1}{2^{\ell-2}}\right)+\left(\frac{1}{4}\right)^{\ell-1}\frac{m}{2}\\
\leq\ &\frac{3}{2}2^{-\ell}m+\left(\frac{1}{4}\right)^{\ell-1}\frac{m}{2},
\end{aligned}$$

and

$$\sum_{s=[2^{-\ell}m]+1}^{[m/2]}\frac{1}{s}<\int_{[2^{-\ell}m]}^{[m/2]}\frac{dt}{t}\leq\log\frac{m/2}{[2^{-\ell}m]}\leq\ell\log 2,$$

since $[2^{-\ell}m]>2^{-\ell-1}m$ for $m\geq 2^{\ell+1}m_0>2^{\ell+1}$. Therefore, from (6.21),

$$\begin{aligned}
\sum_{s=1}^{[m/2]}|r_s|\ &\leq\ \frac{1}{4}\left\{\frac{3}{2}2^{-\ell}m+\left(\frac{1}{4}\right)^{\ell-1}\frac{m}{2}\right\}+K\eta_{\ell-1}\ell\log 2\\
&\leq\ \frac{m}{4}2^{-\ell+1}+K\eta_{\ell-1}\ell\log 2.
\end{aligned}$$

Hence, if $\ell\geq 2$,

$$\begin{aligned}
\frac{2}{m}\left(\frac{1}{4}\right)^{\ell+1}\sum_{s=1}^{[m/2]}|r_s|\ &\leq\ \left(\frac{1}{4}\right)^{\ell+2}+\frac{K}{m}\eta_{\ell-1}\frac{2\ell\log 2}{4^{\ell+1}}\\
&\leq\ \left(\frac{1}{4}\right)^{\ell+2}+\frac{1}{16}\frac{K}{m}\eta_{\ell-1}\eta.
\end{aligned}\tag{6.22}$$

Plainly, (6.22) holds if $\ell=1$.

Now, by applying (6.20) and (6.22) to (6.19), we arrive at

$$\begin{aligned}
|r_m|\ &\leq\ \left(\frac{1}{4}\right)^{\ell+2}+\frac{1}{16}\frac{K}{m}\eta_{\ell-1}\eta+\frac{2}{3}\frac{K}{m}\eta_\ell\eta+\frac{K}{m}\\
&\leq\ \left(\frac{1}{4}\right)^{\ell+2}\frac{K}{m}\eta_{\ell+1}.
\end{aligned}$$

This completes the proof of (6.17) and hence the proof of the theorem. □

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

## 3.7 Elementary Proofs

Based on the tauberian theorem of Bombieri, we can construct elementary proofs of abstract prime number theorems (cf. Zhang [4]).

We begin with an elementary proof of the following formula.

(3.7.1) THEOREM. (Abstract Selberg–Bombieri Formula) *Suppose there exist constants $A > 0$, $q > 1$, $\gamma > 3$, and $c > 0$, such that*

$$|G(n) - Aq^n| \leq cq^n n^{-\gamma}, \quad n = 1, 2, \dots . \tag{7.1}$$

*Then, as $m \to \infty$,*

$$m\bar{\Lambda}(m) + \sum_{r=1}^{m-1} \bar{\Lambda}(r)\bar{\Lambda}(m-r) = 2mq^m + O(q^m), \tag{7.2}$$

*where the $O$–constant depends only on $a$, $q$, $\gamma$, and $c$.*

*Remark.* (7.2) is an analogue of Selberg's formula in classical prime number theory, and was first proved by Bombieri in [1] for an algebraic curve $C$. As is well–known, Selberg's formula is the starting–point of the famous elementary proof of the classical prime number theorem by Selberg and Erdős.

PROOF. The starting–point of our proof is the convolution identity (1.8)

$$(L\bar{\Lambda} + \bar{\Lambda} * \bar{\Lambda}) * G = L^2 G,$$

of Section 3.1 earlier. This implies

$$L\bar{\Lambda} + \bar{\Lambda} * \bar{\Lambda} = L^2 G * G^{-1}, \tag{7.3}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

where $G^{-1}$ is the additive–convolution inverse of $G$. Since

$$\sum_{n=0}^{\infty} G^{-1}(n)y^n = \prod_{m=1}^{\infty}(1-y^m)^{P(m)},$$

it is plain that $|G^{-1}(n)| \leq G(n)$.

The arithmetical function $L^2G$ can be approximated well by a function of the form

$$2(G*T*T)+c_2(G*T)+c_3G,$$

where the function $T$ is defined by setting $T(n)=q^n$, $n=0,1,2,\ldots$, and the coefficients $c_2$ and $c_3$ will be specified later. Write

$$G(n)=Aq^n+a_nq^nn^{-\gamma}, \quad n=1,2,\ldots,$$

where $|a_n| \leq c$ by (7.1). Then

$$(G*T)(n)=q^n\left\{An+(1+\sigma_1)+O\left(\frac{1}{(n+1)^{\gamma-1}}\right)\right\},$$

where $\sigma_1=\sum_{s=1}^{\infty}a_ss^{-\gamma}$, and

$$\begin{aligned}(G*T*T)(n) &= \sum_{0\leq s\leq n} G(s)(T*T)(n-s)\\ &= (n+1)q^n+\sum_{1\leq s\leq n}(n-s+1)q^{n-s}\left(Aq^s+a_sq^ss^{-\gamma}\right)\\ &= q^n\left\{\frac{1}{2}An(n+1)+(n+1)(1+\sigma_1)-\sigma_2+O\left(\frac{1}{(n+1)^{\gamma-2}}\right)\right\},\end{aligned}$$

where $\sigma_2=\sum_{s=1}^{\infty}a_ss^{-\gamma+1}$. If we introduce $R=L^2G-2(G*T*T)-c_2G*T-c_3G$, and choose

$$c_2=-1-\frac{2}{A}(1+\sigma_1), \quad c_3=\frac{1}{A}\left\{-(2+c_2)(1+\sigma_1)+2\sigma_2\right\},$$

then $R(0)=-2-c_2-c_3$ and

$$\begin{aligned}R(n) &= q^n\big\{-(2(1+\sigma_1)+A+c_2A)\,n\\ &\quad +(-(2+c_2)(1+\sigma_1)+2\sigma_2-c_3A)+O(n^{-\gamma+2})\big\}\\ &= q^nO(n^{-\gamma+2})\end{aligned}$$

for $n \geq 1$. Now rewrite (7.3) as

$$L\bar{\Lambda} + \bar{\Lambda} * \bar{\Lambda} = 2T * T + c_2 T + c_3 e + R * G^{-1},$$

where $e$ is the additive-convolution identity defined in Subsection 3.1.1. Then

$$m\bar{\Lambda}(m) + \sum_{r=1}^{m-1} \bar{\Lambda}(r)\bar{\Lambda}(m-r) = 2mq^m + O(q^m),$$

since

$$\begin{aligned} \left|R * G^{-1}(m)\right| &= \left|\sum_{s=0}^{m} R(s)G^{-1}(m-s)\right| \\ &\ll q^m \left(1 + \sum_{s=1}^{m} s^{-\gamma+2}\right) \ll q^m \end{aligned}$$

for $\gamma > 3$. □

We next give an elementary proof of formula (7.7) below, which we shall call *the second analogue of Selberg's formula.* This formula is of independent interest, even though in the further discussion we need only (7.6), which is a consequence of (7.7) and can be proved more easily.

(3.7.2) Lemma. *Let*

$$H(n) := \sum_{k=0}^{n} (-1)^k G(k)G(n-k). \tag{7.4}$$

*If there exist constants $A_1 > 0$, $q > 1$, and $\gamma > 1$ such that*

$$H(2n) = A_1 q^{2n} + O\left(q^{2n} n^{-\gamma}\right) \tag{7.5}$$

*as $n \to \infty$, then*

$$\sum_{s=1}^{n} \frac{\bar{\Lambda}(2s)}{q^{2s}} = n + O(1). \tag{7.6}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

*Furthermore, if (7.5) holds with $\gamma > 3$ then*

$$n\bar{\Lambda}(2n) + \sum_{s=1}^{n} \bar{\Lambda}(2s)\bar{\Lambda}(2n-2s) = 2nq^{2n} + O\left(q^{2n}\right). \tag{7.7}$$

PROOF. First note that

$$\begin{aligned}\sum_{n=0}^{\infty} H(n)y^n &= \sum_{n=0}^{\infty}(-1)^n G(n)y^n \sum_{n=0}^{\infty} G(n)y^n \\ &= \prod_{\substack{m=1\\ m \text{ even}}}^{\infty} (1-y^m)^{-2P(m)} \prod_{\substack{m=1\\ m \text{ odd}}}^{\infty} \left(1-y^{2m}\right)^{-P(m)} \\ &= \prod_{m=1}^{\infty} (1-y^m)^{-\hat{P}(m)},\end{aligned}$$

where

$$\hat{P}(m) = \begin{cases} 0, & \text{if } m \text{ is odd;} \\ 2P(m) + P\left(\frac{m}{2}\right), & \text{if } m = 2k \text{ with } k \text{ odd;} \\ 2P(m), & \text{if } 4 \mid m. \end{cases}$$

Therefore, $H(n) \geq 0$ for all $n$.

Now define arithmetical functions $H_1$ and $\Lambda_1$ by setting $H_1(n) = H(2n)$ and $\Lambda_1(n) = \bar{\Lambda}(2n)$. Then $H_1(n) = A_1(q^2)^n + O\left((q^2)^n n^{-\gamma}\right)$, with $A_1 > 0$ and $q^2 > 1$ by (7.5). It is easily verified that

$$\begin{aligned}&\sum_{n=1}^{\infty} \Lambda_1(n)y^n \sum_{n=0}^{\infty} H_1(n)y^n \\ &\quad = \frac{1}{2}\left\{\sum_{n=1}^{\infty} \bar{\Lambda}(n)\left(y^{\frac{1}{2}}\right)^n + \sum_{n=1}^{\infty} \bar{\Lambda}(n)\left(-y^{\frac{1}{2}}\right)^n\right\} \\ &\quad \times \sum_{n=0}^{\infty} G(n)\left(y^{\frac{1}{2}}\right)^n \sum_{n=0}^{\infty} G(n)\left(-y^{\frac{1}{2}}\right)^n \\ &\quad = \sum_{n=0}^{\infty} nH_1(n)y^n,\end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

or, equivalently,

$$\Lambda_1 * H_1 = LH_1.$$

Therefore, if (7.5) holds with $\gamma > 1$, then $H_1$ satisfies the condition of Theorem 3.3.1, and hence

$$\sum_{k=1}^{n} \frac{\Lambda_1(k)}{(q^2)^k} = \sum_{k=1}^{n} \frac{\bar{\Lambda}(2k)}{q^{2k}} = n + O(1).$$

Furthermore, if (7.5) holds with $\gamma > 3$, then $H_1$ satisfies the conditions of Theorem 3.7.1. Hence

$$n\Lambda_1(n) + \sum_{s=1}^{n-1} \Lambda_1(s)\Lambda_1(n-s) = 2nq^{2n} + O\left(q^{2n}\right),$$

and (7.7) follows. □

We now derive a third version of the abstract prime number theorem. Its proof is elementary.

(3.7.3) THEOREM. *Suppose there exist constants $A > 0$, $B > 0$, $q > 1$, $\gamma > 3$, and $\delta > 1$, such that*

$$G(n) = Aq^n + O\left(q^n n^{-\gamma}\right), \quad n = 1, 2, \ldots \tag{7.8}$$

*and*

$$\sum_{k=0}^{2n} (-1)^k G(k) G(2n-k) = Bq^{2n} + O\left(q^{2n} n^{-\delta}\right), \quad n = 1, 2, \ldots . \tag{7.9}$$

*Then*

$$\bar{\Lambda}(n) = q^n + O\left(\frac{q^n}{n}\right). \tag{7.10}$$

PROOF. The present hypotheses imply, by Theorem 3.7.1 and Lemma 3.7.2, that

$$m\frac{\bar{\Lambda}(m)}{q^m} + \sum_{k=1}^{m-1} \frac{\bar{\Lambda}(k)}{q^k} \frac{\bar{\Lambda}(m-k)}{q^{m-k}} = 2m + O(1)$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

and

$$\sum_{k=1}^{m} \frac{\bar{\Lambda}(2k)}{q^{2k}} = m + O(1).$$

Also, the hypotheses imply, by Theorem 3.3.1 that

$$\sum_{k=1}^{m} \frac{\bar{\Lambda}(k)}{q^{k}} = m + O(1).$$

Let $a_k = \frac{\bar{\Lambda}(k)}{q^k}$. Then the earlier conditions (6.1), (6.2), and (6.3) are satisfied. Thus, (7.10) follows from Theorem 3.6.1. □

*Remark.* The condition (7.9) with $B > 0$ may be regarded as an elementary counterpart of the non–vanishing at $y = -q^{-1}$ of the generating function $Z(y)$. Actually, as in the proof of Lemma 3.7.2, $1 + \sum_{n=1}^{\infty} H(n)y^n = Z(y)Z(-y)$. From Lemma 3.5.3, if $Z(y)$ has a zero at $y = -q^{-1}$, then $H(2n) = o(q^n)$ and hence $B = 0$ in (7.9). Conversely, if $Z(y)$ has no zero at $y = -q^{-1}$, then $Z(y)Z(-y)$ has a pole of order one at $y = q^{-1}$, and so (7.9) with $B > 0$ follows.

We can deduce Theorem 3.5.6 from Theorem 3.7.3 by an elementary argument:

(3.7.4) PROPOSITION. *Assume the conditions of Theorem 3.5.6. Then (5.5) implies (7.9) with a constant $B > 0$.*

PROOF. The conditions of Theorem 3.5.6 imply $G(n) = Aq^n + O_\nu(q^{\nu n})$ for each $\nu > \frac{1}{2}$. Actually,

$$G(n) = \frac{1}{2\pi i} \int_{|y|=r} \frac{Z(y)}{y^{n+1}}\, dy,$$

where $0 < r < q^{-1}$. Now, $Z(y)$ has an analytic continuation in the disk $\{|y| < q^{-\frac{1}{2}}\}$, for convenience, denoted by the same notation $Z(y)$, which is

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

a meromorphic function with only singularity being a simple pole at $y = q^{-1}$. If we shift the integration path to the circle $\{|y| = q^{-\nu}\}$ with any $\nu > \frac{1}{2}$, then we obtain

$$\begin{aligned} G(n) &= A_1 q^{n+1} + \frac{1}{2\pi i} \int_{|y|=q^{-\nu}} \frac{Z(y)}{y^{n+1}}\, dy \\ &= A_1 q^{n+1} + O_\nu\left(q^{\nu n}\right), \end{aligned}$$

where $A_1 = \operatorname{Res}_{y=q^{-1}} Z(y)$, since $Z(y)$ is bounded on the circle $\{|y| = q^{-\nu}\}$.

We first show that there exists a constant $B$ such that

$$H(2n) = Bq^{2n} + O_\nu\left(q^{2\nu n}\right) \tag{7.11}$$

for each $\nu > \frac{1}{2}$. Let $G(n) = Aq^n + a_n q^{n/2}$, $n = 1, 2, \dots$ . Then $a_n = O_{\nu_0}\left(q^{\left(\nu_0 - \frac{1}{2}\right)n}\right)$ with $\nu_0 = \frac{\nu + \frac{1}{2}}{2} < \nu < 1$. We have

$$\begin{aligned} H(2n) &= 2G(2n) + \sum_{k=1}^{2n-1} (-1)^k G(k) G(2n-k) \\ &= (2A - A^2) q^{2n} + 2Aq^{2n} \sum_{k=1}^{2n-1} (-1)^k a_k q^{-k/2} \\ &\quad + q^n \sum_{k=1}^{2n-1} (-1)^k a_k a_{2n-k} + 2a_{2n} q^n. \end{aligned}$$

Let $\sigma = \sum_{k=1}^{\infty} (-1)^k a_k q^{-k/2}$. Then

$$\begin{aligned} &\sum_{k=1}^{2n-1} (-1)^k a_k q^{-k/2} = \sigma - \sum_{k=2n}^{\infty} (-1)^k a_k q^{-k/2} \\ &\quad = \sigma + \sum_{k=2n}^{\infty} O_{\nu_0}\left(q^{-(1-\nu_0)k}\right) = \sigma + O_{\nu_0}\left(q^{-(2-2\nu_0)n}\right). \end{aligned}$$

Also,

$$\sum_{k=1}^{2n-1} (-1)^k a_k a_{2n-k} = O_{\nu_0}\left(q^{(2\nu_0 - 1)n} n\right).$$

Hence

$$H(2n) = (2A - A^2 + 2A\sigma)q^{2n} + O_{\nu_0}\left(q^{2\nu_0 n}n\right),$$

and (7.11) follows with $B = 2A - A^2 + 2A\sigma$.

Now, assume (5.5). We claim that $B > 0$. Actually, $B \geq 0$ since all $H(n) \geq 0$, from the proof of Lemma 3.7.2. Suppose the claim is not true, so that $B = 0$. Then

$$\sum_{n=0}^{\infty} H(n)x^n = Z(x)Z(-x)$$

is holomorphic for $-q^{-\frac{1}{2}} < x < q^{-\frac{1}{2}}$, by (7.11). As in the proof of Theorem 3.5.6, we have

$$Z(x)Z(-x) = g(x)Z(x^2), \quad |x| < q^{-1},$$

where

$$g(x) = \prod_{\substack{n=1 \\ n \text{ even}}}^{\infty} \left(\frac{1+x^n}{1-x^n}\right)^{P(n)}.$$

Note that $Z(x^2) \neq 0$ for $-q^{-\frac{1}{2}} < x < q^{-\frac{1}{2}}$, and hence $g(x)$ is holomorphic for $-q^{-\frac{1}{2}} < x < q^{-\frac{1}{2}}$ too. The same argument as for the second part in the proof of Theorem 3.5.7 applies again, and we conclude that

$$\left(1 - q^{-\frac{1}{2}}x\right) \ll Z(x)Z(-x),$$

which contradicts (5.5). □

Since (5.5) implies (7.9) with $B > 0$, by Theorem 3.7.3, the abstract prime number theorem holds. Then, by Theorem 3.4.1, $Z(y)$ has no zeros on the circle $|y| = q^{-1}$. This gives another proof of Theorem 3.5.6.

One can also deduce Theorem 3.5.1 from Theorem 3.7.3 by an elementary argument:

(3.7.5) PROPOSITION. *The condition (5.1) implies (7.9) with a constant $B > 0$.*

PROOF. We first show that there exist a constant $B$ such that

$$H(2n) = Bq^{2n} + o(q^n)$$

as $n \to \infty$. Let $G(n) = Aq^n + a_n q^{n/2}$. Then (5.1) implies $\sum_{n=1}^{\infty} a_n^2 < \infty$ and $a_n \to 0$ as $n \to \infty$. Hence

$$\begin{aligned}\sum_{k=1}^{2n-1}(-1)^k a_k a_{2n-k} &= 2\sum_{k=1}^{n-1}(-1)^k a_k a_{2n-k} + (-1)^n a_n^2 \\ &= o(1)\end{aligned}$$

as $n \to \infty$, since, by the Cauchy–Schwarz inequality,

$$\left|\sum_{k=1}^{n-1}(-1)^k a_k a_{2n-k}\right| \le \left(\sum_{k=1}^{n-1} a_k^2\right)^{\frac{1}{2}} \left(\sum_{k=1}^{n-1} a_{2n-k}^2\right)^{\frac{1}{2}} \to 0.$$

Thus

$$\begin{aligned}H(2n) &= 2G(2n) + \sum_{k=1}^{2n-1}(-1)^k G(k)G(2n-k) \\ &= 2\left(Aq^{2n} + a_{2n}q^n\right) \\ &\quad + \sum_{k=1}^{2n-1}(-1)^k\left(Aq^k + a_k q^{k/2}\right)\left(Aq^{2n-k} + a_{2n-k}q^{n-k/2}\right) \\ &= \left(2A - A^2 + 2A\sigma\right)q^{2n} + o(q^n)\end{aligned}$$

where $\sigma = \sum_{k=1}^{\infty}(-1)^k a_k q^{-k/2}$.

We claim $B = 2A - A^2 + 2A\sigma > 0$. Suppose on the contrary that $B = 0$. Then $H(2n) = o(q^n)$. As in the proof of Theorem 3.5.1, we write

$$\sum_{n=0}^{\infty} H(n)x^n = Z(x)Z(-x) = \prod_{\substack{m=1 \\ m \text{ even}}}^{\infty}\left(\frac{1+x^m}{1-x^m}\right)^{P(m)} Z(x^2)$$

for $-q^{-1} < x < q^{-1}$, and

$$Z(x^2) = \sum_{n=0}^{\infty} G_1(n)x^n,$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

$$\prod_{\substack{m=1\\ m \text{ even}}}^{\infty} \left(\frac{1+x^m}{1-x^m}\right)^{P(m)} = \sum_{n=0}^{\infty} G_2(n)x^n.$$

Then $G_2(n) \geq 0$ and

$$G_1(n) = \begin{cases} G\left(\frac{n}{2}\right), & \text{if } n \text{ is even,} \\ 0, & \text{if } n \text{ is odd.} \end{cases}$$

As in the proof of Theorem 3.5.1, it follows that

$$\liminf_{n\to\infty} q^{-n}H(2n) \geq \lim_{n\to\infty} q^{-n}G(n) = A > 0;$$

this contradicts $H(2n) = o(q^n)$. □

Theorem 3.7.3 has some advantages over Theorems 3.5.1 and 3.5.6. It does not assume an analytic continuation of $Z(y)$ in the disk $\left\{|y| < q^{-\frac{1}{2}}\right\}$ to a meromorphic function with the only singularity being a pole of order one at $y = q^{-1}$, or an essentially equivalent condition on $G(n)$. Instead, the condition (7.8) is very weak. This condition guarantees only the convergence and second-order smoothness of $Z(y)$ on the circle $|y| = q^{-1}$.

Finally, by combining Theorem 3.7.2 and Theorem 3.4.5, we obtain the following abstract prime number theorem.

(3.7.6) THEOREM. *If the condition (7.8) of Theorem 3.7.3 is replaced by Axiom $\mathcal{A}^{\#}$, then*

$$\bar{\Lambda}(n) = q^n + O\left(q^{\theta n}\right)$$

*holds for some $\theta$ with* $0 < \theta < 1$.

*Remark.* An elementary proof of Theorems 3.7.3 and 3.7.6 can also be constructed on the basis of Lemma 3.6.2 and a lemma of Wirsing (see Wirsing [1] and Chandrasekharan [1]). We shall not introduce this proof here, but interested readers may read Zhang [4].

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

## 3.8 Two Analytical Examples

In this section, we shall give two analytical examples (cf. Zhang [1]). The first one shows that the Theorems 3.5.1 and 3.5.6 are sharp and that, in the general case, a positive lower bound for $\bar{\Lambda}(n)q^{-n}$ does not exist, even with $G(n)$ subject to rather restrictive conditions. (In these examples, the word *formal* is used to indicate that actual arithmetical semigroups are only defined *implicitly* in terms of suitable analytical parameters, and not in terms of any pre-existing algebraic or other natural context.)

(3.8.1) EXAMPLE. Let $q \geq 2$ be a positive integer. Let

$$2q^k \equiv r_k \bmod k, \quad 0 \leq r_k < k,$$

for $k = 1, 2, \ldots$. Formally set

$$P(k) = \begin{cases} \frac{1}{k}\left(2q^k - r_k\right) + 1, & \text{if } k \text{ is odd,} \\ 1, & \text{if } k \text{ is even.} \end{cases}$$

(We could instead put $P(k) = 0$ for $k$ even.) Then the $P(k)$ for $k = 1, 2, \ldots,$ are all positive integers, and $kP(k) \ll q^k$. Note that $kP(k) > 2q^k$, if $k$ is odd. Therefore, the corresponding formal von Mangoldt function satisfies

$$\bar{\Lambda}(n) = \sum_{k|n} kP(k) = \begin{cases} 2q^n + c_n, & \text{if } n \text{ is odd,} \\ 2q^{\frac{n}{2}} + c_n, & \text{if } n = 2k \text{ with } k \text{ odd,} \\ c_n, & \text{if } 4 \mid n, \end{cases} \tag{8.1}$$

where $c_n > 0$, and $c_n \ll q^{\frac{n}{3}} \log n$. Thus, the earlier abstract prime number theorems do not hold here.

It is easily verified that the corresponding formal generating function

$$Z(y) = \prod_{m=1}^{\infty} (1 - y^m)^{-P(m)}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

converges absolutely in the disk $\{|y| < q^{-1}\}$.

(3.8.2) PROPOSITION. *If we formally write*

$$Z(y) = 1 + \sum_{n=1}^{\infty} G(n) y^n$$

*then the $G(n)$ are all positive integers, and there exists a positive constant $A$ such that*

$$q^{\frac{n}{2}} n^{-\frac{1}{2}} \ll |G(n) - Aq^n| \ll q^{\frac{n}{2}} n^{-\frac{1}{2}} \tag{8.2}$$

*holds for $n$ sufficiently large. Moreover, $Z(y)$ has a zero of order one at $y = -q^{-1}$.*

We divide the proof of Proposition 3.8.2 into several lemmas. Let $\mathcal{D}$ be the domain formed by cutting the complex plane along the real axis from $-\infty$ to $-q^{-\frac{1}{2}}$, and from $q^{-\frac{1}{2}}$ to $+\infty$, and along the imaginary axis from $-i\infty$ to $-iq^{-\frac{1}{2}}$, and from $iq^{-\frac{1}{2}}$ to $i\infty$.

(3.8.3) LEMMA. *The above function $Z(y)$ has an analytic continuation in $\mathcal{D} \cap \left\{|y| < q^{-\frac{1}{3}}\right\}$ as a single-valued meromorphic function with the only singularity being a pole of order one at $y = q^{-1}$, and the only zero of order one at $y = -q^{-1}$.*

PROOF. By (8.1), we have

$$\frac{y\dfrac{d}{dy}Z(y)}{Z(y)} = \Lambda^{\#}(y) = \frac{2qy}{1-(qy)^2} + \frac{2qy^2}{1-(qy^2)^2} + yf(y), \quad |y| < q^{-1},$$

where the function $f(y) := \sum_{n=1}^{\infty} c_n y^{n-1}$ is holomorphic in the disk $\left\{|y| < q^{-\frac{1}{3}}\right\}$. It turns out that

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

$$Z(y) = \frac{1+qy}{1-qy}\left(\frac{1+qy^2}{1-qy^2}\right)^{\frac{1}{2}} e^{F(y)}, \quad |y| < q^{-1}, \tag{8.3}$$

where the function $F(y) = \sum_{n=1}^{\infty} c_n n^{-1} y^n$ is, like $f(y)$, holomorphic in the disk $\left\{|y| < q^{-\frac{1}{3}}\right\}$. Moreover, in (8.3), the function

$$M(y) := \left(\frac{1+qy^2}{1-qy^2}\right)^{\frac{1}{2}}$$

is the single-valued branch with $M(0) = 1$ of the associated multiple-valued function. The domain where $M(y)$ is holomorphic is $\mathcal{D}$. □

We have

$$G(n) = \frac{1}{2\pi i}\int_{|y|=r_1} \frac{Z(y)}{y^{n+1}}\,dy,$$

where $0 < r_1 < q^{-1}$. From Lemma 3.8.3, if we shift the integration contour to the circle $|y| = q^{-\frac{1}{2}-\varepsilon}$ then we shall obtain

$$\begin{aligned} G(n) &= -\operatorname*{Res}_{y=q^{-1}} \frac{Z(y)}{y^{n+1}} + \frac{1}{2\pi i}\int_{|y|=q^{-\frac{1}{2}-\varepsilon}} Z(y) y^{-n-1} dy \\ &= 2\left(\frac{q+1}{q-1}\right)^{\frac{1}{2}} e^{F(q^{-1})} q^n + O_\varepsilon\left(q^{\left(\frac{1}{2}+\varepsilon\right)n}\right). \end{aligned}$$

However, it is possible to get the more accurate estimate (8.2) by introducing a complicated integration path $\mathcal{C}$ (Fig. 1)

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

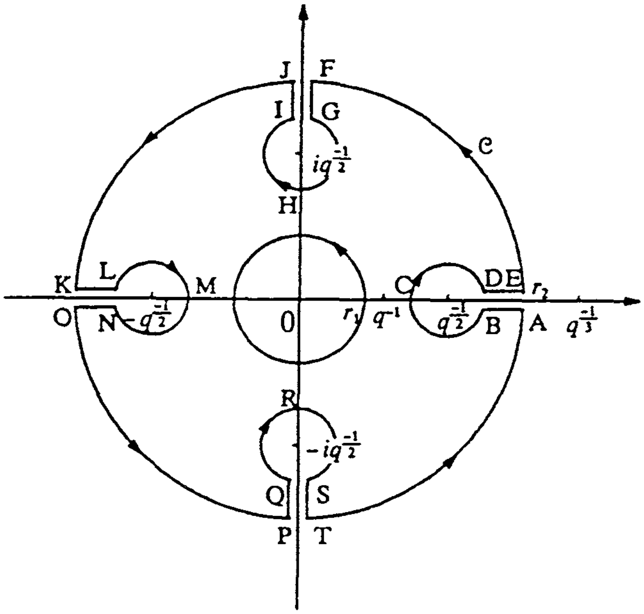

Figure 1

(3.8.4) Lemma. *We have*

$$G(n) = Aq^n + \frac{1}{\pi}\left(I_n^{(1)} + I_n^{(2)} + I_n^{(3)} + I_n^{(4)}\right) + O_\varepsilon\left(q^{\left(\frac{1}{3}+\varepsilon\right)n}\right), \tag{8.4}$$

*where* $A = 2\left(\frac{q+1}{q-1}\right)^{\frac{1}{2}} e^{F(q^{-1})}$, *and*

$$I_n^{(1)} = -q^{\frac{n}{2}} \int_1^{q^{\frac{1}{6}-\varepsilon}} \alpha^{-n-1} \left(\frac{\alpha^2+1}{\alpha^2-1}\right)^{\frac{1}{2}} \frac{q^{\frac{1}{2}}\alpha+1}{q^{\frac{1}{2}}\alpha-1} \exp\left\{F\left(q^{-\frac{1}{2}}\alpha\right)\right\} d\alpha,$$

$$I_n^{(2)} = (-1)^{n+1} q^{\frac{n}{2}} \int_1^{q^{\frac{1}{6}-\varepsilon}} \alpha^{-n-1} \left(\frac{\alpha^2+1}{\alpha^2-1}\right)^{\frac{1}{2}} \frac{q^{\frac{1}{2}}\alpha+1}{q^{\frac{1}{2}}\alpha-1} \exp\left\{F\left(-q^{-\frac{1}{2}}\alpha\right)\right\} d\alpha,$$

$$I_n^{(3)} = \frac{q^{\frac{n}{2}}}{i^n} \int_1^{q^{\frac{1}{6}-\varepsilon}} \alpha^{-n-1} \left(\frac{\alpha^2-1}{\alpha^2+1}\right)^{\frac{1}{2}} \frac{1+iq^{\frac{1}{2}}\alpha}{1-iq^{\frac{1}{2}}\alpha} \exp\left\{F\left(iq^{-\frac{1}{2}}\alpha\right)\right\} d\alpha,$$

$$I_n^{(4)} = (-1)^n \frac{q^{\frac{n}{2}}}{i^n} \int_1^{q^{\frac{1}{6}-\varepsilon}} \alpha^{-n-1} \left(\frac{\alpha^2-1}{\alpha^2+1}\right)^{\frac{1}{2}} \frac{1-iq^{\frac{1}{2}}\alpha}{1+iq^{\frac{1}{2}}\alpha} \exp\left\{F\left(-iq^{-\frac{1}{2}}\alpha\right)\right\} d\alpha.$$

PROOF. With reference to Figure 1, define an integration contour $\mathcal{C}$ which consists of the circle $|y| = r_2$ with $r_2 = q^{-\frac{1}{3}-\varepsilon}$ cut at points $\pm q^{-\frac{1}{3}-\varepsilon}$, $\pm iq^{-\frac{1}{3}-\varepsilon}$, the line segments $AB$ and $NO$ on the lower edge of the cut of $\mathcal{D}$ along the real axis, the line segments $DE$ and $KL$ on the upper edge, the segments $FG$ and $ST$ on the right edge of the cut along the imaginary axis, the segments $IJ$ and $PQ$ on the left edge, and the small circles $BCD$, $GHI$, $LMN$, and $QRS$ centered at $q^{-\frac{1}{2}}$, $iq^{-\frac{1}{2}}$, $-q^{-\frac{1}{2}}$, and $-iq^{-\frac{1}{2}}$ respectively with the same radius $\eta$ sufficiently small. Thus we have

$$G(n) = Aq^n + \frac{1}{2\pi i} \int_{\mathcal{C}} \frac{Z(y)}{y^{n+1}} dy \tag{8.5}$$

with $A = 2\left(\frac{q+1}{q-1}\right)^{\frac{1}{2}} \exp\{F(q^{-1})\} > 0$. We shall estimate the last integral on each part of $\mathcal{C}$ separately.

It is easy to see that the integrals on the arcs $EF$, $JK$, $OP$, and $TA$ are all $O_\varepsilon\left(q^{\left(\frac{1}{3}+\varepsilon\right)n}\right)$. To evaluate the integrals on the line segments, we now consider the function $M(y) = \left(\frac{1+qy^2}{1-qy^2}\right)^{\frac{1}{2}}$.

Note that $M(y)$ acquires a factor $-1$ when $y$ jumps from $AB$ to $DE$ and so does the integrand $Z(y)y^{-n-1}$. Also note that the argument of $1 - q^{\frac{1}{2}}y$ increases by $-\pi$, and hence the argument of $M(y)$ increases by $\frac{\pi}{2}$, when $y$ tours from $C$ to $D$ along the circle $BCD$. Therefore

$$\left(\int_{AB} + \int_{DE}\right) \frac{Z(y)}{y^{n+1}} dy = 2\int_{DE} \frac{Z(y)}{y^{n+1}} dy$$

$$= 2\int_{q^{-\frac{1}{2}}+\eta}^{q^{-\frac{1}{3}-\varepsilon}} i\frac{1}{y^{n+1}} \frac{1+qy}{1-qy} \left(\frac{qy^2+1}{qy^2-1}\right)^{\frac{1}{2}} e^{F(y)} dy. \tag{8.6}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Similarly,

$$\left(\int_{KL}+\int_{NO}\right)\frac{Z(y)}{y^{n+1}}\,dy = 2\int_{NO}\frac{Z(y)}{y^{n+1}}\,dy$$

$$= 2\int_{-q^{-\frac{1}{2}}-\eta}^{-q^{-\frac{1}{3}-\epsilon}} i\frac{1}{y^{n+1}}\,\frac{1+qy}{1-qy}\left(\frac{qy^2+1}{qy^2-1}\right)^{\frac{1}{2}} e^{F(y)}dy \qquad (8.7)$$

$$\left(\int_{FG}+\int_{IJ}\right)\frac{Z(y)}{y^{n+1}}\,dy = 2\int_{IJ}\frac{Z(y)}{y^{n+1}}\,dy$$

$$= 2\int_{q^{-\frac{1}{2}}+\eta}^{q^{-\frac{1}{3}-\epsilon}} \frac{-1}{(it)^{n+1}}\,\frac{1+itq}{1-itq}\left(\frac{qt^2-1}{qt^2+1}\right)^{\frac{1}{2}} e^{F(it)}dt, \qquad (8.8)$$

and

$$\left(\int_{PQ}+\int_{ST}\right)\frac{Z(y)}{y^{n+1}}\,dy = 2\int_{ST}\frac{Z(y)}{y^{n+1}}\,dy$$

$$= 2\int_{-q^{-\frac{1}{2}}-\eta}^{-q^{-\frac{1}{3}-\epsilon}} \frac{-1}{(it)^{n+1}}\,\frac{1+itq}{1-itq}\left(\frac{qt^2-1}{qt^2+1}\right)^{\frac{1}{2}} e^{F(it)}dt. \qquad (8.9)$$

Moreover, on the circle $BCD$, if we set $y - q^{-\frac{1}{2}} = \eta e^{i\theta}$, $0 \le \theta \le 2\pi$, then

$$\left(1 - q^{\frac{1}{2}}y\right)^{-\frac{1}{2}} = iq^{-\frac{1}{4}}\eta^{-\frac{1}{2}}e^{-i\theta/2},$$

and hence

$$\int_{BCD}\frac{Z(y)}{y^{n+1}}dy \to 0 \text{ as } \eta \to \infty,$$

since the circumference of $BCD$ is $2\pi\eta$. Similarly, the integrals on the small circles $GHI$, $LMN$, and $QRS$ tend to zero as $\eta \to 0$ too.

From (8.6), (8.7), (8.8), and (8.9), if we let $\eta \to 0$ in (8.5) and take the limit on the right-hand side then we obtain

$$G(n) = Aq^n + \frac{1}{\pi}\left(I_n^{(1)} + I_n^{(2)} + I_n^{(3)} + I_n^{(4)}\right) + O_\varepsilon\left(q^{\left(\frac{1}{3}+\varepsilon\right)n}\right),$$

where

$$
\begin{aligned}
I_n^{(1)} &= \int_{q^{-\frac{1}{2}}}^{q^{-\frac{1}{3}-\epsilon}} \frac{1}{y^{n+1}} \frac{1+qy}{1-qy} \left(\frac{qy^2+1}{qy^2-1}\right)^{\frac{1}{2}} e^{F(y)} dy, \\
I_n^{(2)} &= \int_{-q^{-\frac{1}{2}}}^{-q^{-\frac{1}{3}-\epsilon}} \frac{1}{y^{n+1}} \frac{1+qy}{1-qy} \left(\frac{qy^2+1}{qy^2-1}\right)^{\frac{1}{2}} e^{F(y)} dy, \\
I_n^{(3)} &= \int_{q^{-\frac{1}{2}}}^{q^{-\frac{1}{3}-\epsilon}} \frac{1}{i^n t^{n+1}} \frac{1+itq}{1-itq} \left(\frac{qt^2-1}{qt^2+1}\right)^{\frac{1}{2}} e^{F(it)} dt, \\
I_n^{(4)} &= \int_{-q^{-\frac{1}{2}}}^{-q^{-\frac{1}{3}-\epsilon}} \frac{1}{i^n t^{n+1}} \frac{1+itq}{1-itq} \left(\frac{qt^2-1}{qt^2+1}\right)^{\frac{1}{2}} e^{F(it)} dt.
\end{aligned}
$$

Now if we make the substitution $y = q^{-\frac{1}{2}}\alpha$ in $I_n^{(1)}$, $t = q^{-\frac{1}{2}}\alpha$ in $I_n^{(3)}$, $y = -q^{-\frac{1}{2}}\alpha$ in $I_n^{(2)}$, and $t = -q^{-\frac{1}{2}}\alpha$ in $I_n^{(4)}$, then the required expressions of $I_n^{(1)}$, $I_n^{(2)}$, $I_n^{(3)}$, and $I_n^{(4)}$ follow. □

(3.8.5) LEMMA. *We have*

$$n^{-\frac{1}{2}} \ll \int_1^a \alpha^{-n-1}(\alpha-1)^{-\frac{1}{2}} d\alpha \ll n^{-\frac{1}{2}},$$

*where $a$ is an arbitrary constant with $a > 1$.*

PROOF. Actually we have

$$
\begin{aligned}
\int_1^{1+\frac{1}{n}} \alpha^{-n-1}(\alpha-1)^{-\frac{1}{2}} d\alpha &\geq \left(\frac{1}{n}\right)^{-\frac{1}{2}} \int_1^{1+\frac{1}{n}} \alpha^{-n-1} d\alpha \\
&> n^{-\frac{1}{2}}(1-2e^{-1}),
\end{aligned}
$$

and, by integration by parts,

$$\int_1^{1+\frac{1}{n}} \alpha^{-n-1}(\alpha-1)^{-\frac{1}{2}} d\alpha$$

$$\begin{aligned}&= 2\left(\frac{1}{n}\right)^{-\frac{1}{2}}\left(1+\frac{1}{n}\right)^{-n-1} + 2(n+1)\int_1^{1+\frac{1}{n}}(\alpha-1)^{-\frac{1}{2}}\alpha^{-n-2}d\alpha\\ &\le 2n^{-\frac{1}{2}} + 2n^{-\frac{1}{2}}(n+1)\int_1^{1+\frac{1}{n}}\alpha^{-n-2}d\alpha\\ &\ll n^{-\frac{1}{2}}.\end{aligned}$$

Also,

$$\int_{1+\frac{1}{n}}^{a}\alpha^{-n-1}(\alpha-1)^{-\frac{1}{2}}d\alpha \le \left(\frac{1}{n}\right)^{-\frac{1}{2}}\int_{1+\frac{1}{n}}^{a}\alpha^{-n-1}d\alpha \le n^{-\frac{1}{2}}. \quad \square$$

*Proof of Proposition 3.8.2* By Lemma 3.8.4, it remains to show that

$$q^{\frac{n}{2}}n^{-\frac{1}{2}} \ll \left|I_n^{(1)}+I_n^{(2)}+I_n^{(3)}+I_n^{(4)}\right| \ll q^{\frac{n}{2}}n^{-\frac{1}{2}} \tag{8.10}$$

holds for $n$ sufficiently large. We write

$$\begin{aligned}I_n^{(1)}+I_n^{(2)} &= q^{\frac{n}{2}}\int_1^{q^{\frac{1}{6}-\epsilon}}\alpha^{-n-1}\left(\frac{\alpha^2+1}{\alpha^2-1}\right)^{\frac{1}{2}}\Bigg(-\frac{q^{\frac{1}{2}}\alpha+1}{q^{\frac{1}{2}}\alpha-1}\exp\left\{F(q^{-\frac{1}{2}}\alpha)\right\}\\ &\qquad + (-1)^{n+1}\frac{q^{\frac{1}{2}}\alpha-1}{q^{\frac{1}{2}}\alpha+1}\exp\left\{F(-q^{-\frac{1}{2}}\alpha)\right\}\Bigg)d\alpha.\end{aligned}$$

Hence, by Lemma 3.8.5,

$$\left|I_n^{(1)}+I_n^{(2)}\right| \ll q^{\frac{n}{2}}\int_1^{q^{\frac{1}{6}-\epsilon}}\alpha^{-n-1}(\alpha-1)^{-\frac{1}{2}}d\alpha \ll q^{\frac{n}{2}}n^{-\frac{1}{2}}.$$

Moreover, we have

$$\begin{aligned}&I_n^{(1)}+I_n^{(2)}\\ &\quad\le q^{\frac{n}{2}}\int_1^{q^{\frac{1}{6}-\epsilon}}\alpha^{-n-1}\left(\frac{\alpha^2+1}{\alpha^2-1}\right)^{\frac{1}{2}}\left(-\frac{q^{\frac{1}{2}}\alpha+1}{q^{\frac{1}{2}}\alpha-1}+\frac{q^{\frac{1}{2}}\alpha-1}{q^{\frac{1}{2}}\alpha+1}\right)\exp\left\{F(q^{-\frac{1}{2}}\alpha)\right\}d\alpha\\ &\quad= -q^{\frac{n}{2}}\int_1^{q^{\frac{1}{6}-\epsilon}}\alpha^{-n-1}\left(\frac{\alpha^2+1}{\alpha^2-1}\right)^{\frac{1}{2}}\frac{4q^{\frac{1}{2}}\alpha}{q\alpha^2-1}\exp\left\{F(q^{-\frac{1}{2}}\alpha\right\}d\alpha,\end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

since the coefficients of $F(y) = \sum_{n=1}^{\infty} c_n n^{-1} y^n$ are all positive, and hence $F(q^{-\frac{1}{2}}\alpha) \geq F(-q^{-\frac{1}{2}}\alpha)$. It follows that

$$I_n^{(1)} + I_n^{(2)} \leq -cq^{\frac{n}{2}} n^{-\frac{1}{2}}$$

for some constant $c > 0$, by Lemma 3.8.5. Therefore

$$q^{\frac{n}{2}} n^{-\frac{1}{2}} \ll \left| I_n^{(1)} + I_n^{(2)} \right| \ll q^{\frac{n}{2}} n^{-\frac{1}{2}}.$$

Finally, we have

$$\left| I_n^{(3)} + I_n^{(4)} \right| \ll q^{\frac{n}{2}} \int_1^{q^{\frac{1}{6}-\epsilon}} \alpha^{-n-1} da \ll q^{\frac{n}{2}} n^{-1}.$$

This proves (8.10) and completes the proof of Proposition 3.8.2. □

Example 3.8.1 also serves other purposes and we shall revisit it in Chapter 5 below.

We now turn to the second example of this section. A famous monograph of A. Weil [1] gave the first proof of the so-called "Riemann hypothesis for algebraic curves over Galois fields". We may also consider an analogue of the Riemann hypothesis for additive arithmetical semigroups:

Suppose $\mathcal{G}$ is an additive arithmetical semigroup satisfying Axiom $\mathcal{A}^{\#}$, for which

$$G(n) = Aq^n + O\left(q^{\nu n}\right), \quad n = 1, 2, \ldots \tag{8.11}$$

for constants $q > 1$, $A > 0$, and $\nu$ with $0 \leq \nu < \frac{1}{2}$. Then the associated generating function $Z(y)$ has an analytic continuation in the disk $\{|y| < q^{-\nu}\}$ as a meromorphic function with the only singularity being a simple pole at $y = q^{-1}$. The "Riemann hypothesis for $\mathcal{G}$" will be understood to be the assertion that $Z(y)$ has no zeros in the disk $\left\{|y| < q^{-\frac{1}{2}}\right\}$. A problem (cf. S.D. Cohen [1]) relevant to this hypothesis is to describe more precisely in terms of $\nu$ the quantity $\theta$ in the remainder term of the abstract prime number theorem, see Theorem 3.5.5. The following example shows that there

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

is not too much we can say about $\theta$ in terms of $\nu$, and that, in the general case, the Riemann hypothesis is not true for arbitrary additive arithmetical semigroups.

(3.8.6) EXAMPLE. Let $q$ and $\eta$ be real numbers with $q > 1$, and $1 > \eta > 0$. Let $k$ be a positive integer, and $k \geq 2$. Set

$$S_\ell(m) = \begin{cases} \displaystyle\sum_{r \mid \frac{m}{\ell}} q^r \mu\left(\frac{m}{\ell r}\right), & \text{if } \ell \mid m, \\ 0, & \text{if } \ell \nmid m, \end{cases}$$

for $m = 1, 2, \ldots$, where $\mu$ is the classical Möbius function on $\mathbb{N}$. Let $q_1 = q^{1-\eta}$. Let

$$S_m = \begin{cases} [q^m], & \text{if } m < m_0, \\ \left[ q^m - \displaystyle\sum_{r \mid m} q_1^r \mu\left(\frac{m}{r}\right) - \sum_{\ell=2}^{k} S_\ell(m) \right], & \text{if } m \geq m_0, \end{cases}$$

for $m = 1, 2, \ldots$, where $[a]$ denotes the largest integer not exceeding $a$, and $m_0$ is sufficiently large. Plainly,

$$\left| \sum_{r \mid m} q_1^r \mu\left(\frac{m}{r}\right) \right| \leq \sum_{s=1}^{m} q_1^s < \frac{q_1^{m+1}}{q_1 - 1},$$

and, if $\ell \mid m$,

$$|s_\ell(m)| = \left| \sum_{r \mid \frac{m}{\ell}} q^r \mu\left(\frac{m}{\ell r}\right) \right| \leq \sum_{s=1}^{m/\ell} q^s < \frac{q^{\frac{m}{\ell}+1}}{q-1}.$$

Therefore,

$$\begin{aligned} & q^m - \sum_{r \mid m} q_1^r \mu\left(\frac{m}{r}\right) - \sum_{\ell=2}^{k} S_\ell(m) \\ & \quad > q^m \left( 1 - \frac{1}{(q_1 - 1) q^{\eta m - 1}} - \frac{k}{(q-1) q^{\frac{m}{2} - 1}} \right) > 1, \end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

if $m \geq m_0(\eta, k)$, and hence the $S_m$ are positive integers. Moreover, $S_m \leq 2q^m$.

Let

$$S_m \equiv r_m \bmod m, \quad 0 \leq r_m < m$$

for $m = 1, 2, \ldots$. Set formally

$$P(m) = \frac{1}{m}(S_m - r_m + m).$$

Then the $P(m)$, $m = 1, 2, \ldots$, are all positive integers, and

$$mP(m) = q^m + m - r_m + \theta_m,$$

with $|\theta_m| < 1$ if $m < m_0$, and

$$mP(m) = q^m - \sum_{r|m} q_1^r \mu\left(\frac{m}{r}\right) - \sum_{\ell=2}^{k} S_\ell(m) + m - r_m + \theta_m,$$

with $|\theta_m| < 1$ if $m \geq m_0$.

The associated formal generating function is, for $|y| < q^{-1}$,

$$\begin{aligned} Z(y) &= \prod_{m=1}^{\infty} (1 - y^m)^{-P(m)} = \exp\left\{\sum_{n=1}^{\infty} \frac{1}{n}\left(\sum_{m|n} mP(m)\right) y^n\right\} \\ &= \exp\left\{\sum_{n=1}^{\infty} \frac{1}{n}\left(\sum_{m|n}\left(q^m - \sum_{r|m} q_1^r \mu\left(\frac{m}{r}\right) - \sum_{\ell=2}^{k} S_\ell(m)\right)\right) y^n \right. \\ &\qquad \left. +F(y)\right\}, \end{aligned} \tag{8.12}$$

where

$$F(y) = \sum_{n=1}^{\infty} \frac{1}{n}\left(\sum_{m|n} (m - r_m + \theta_m)\right.$$

$$+ \sum_{\substack{m|n \\ m<m_0}} \left( \sum_{r|m} q_1^r \mu\left(\frac{m}{r}\right) + \sum_{\ell=2}^{k} S_\ell(m) \right) \Bigg) y^n$$

$$= \sum_{n=1}^{\infty} \frac{1}{n} \left( O(n^{1+\varepsilon}) + O(q^{m_0}) \right) y^n$$

is holomorphic in the disk $\{|y| < 1\}$. Note that

$$\sum_{n=1}^{\infty} \frac{1}{n} \left( \sum_{m|n} q^m \right) y^n = \sum_{s=1}^{\infty} \frac{1}{s} \log\,(1 - qy^s)^{-1}. \tag{8.13}$$

Moreover, since

$$\sum_{m|n} \sum_{r|m} q_1^r \mu\left(\frac{m}{r}\right) = q_1^n,$$

we have

$$\sum_{n=1}^{\infty} \frac{1}{n} \left( \sum_{m|n} \left( - \sum_{r|m} q_1^r \mu\left(\frac{m}{r}\right) \right) \right) y^n$$

$$= - \sum_{n=1}^{\infty} \frac{1}{n} (q_1 y)^n = \log(1 - q_1 y). \tag{8.14}$$

Similarly, if $\ell \mid n$, then

$$\sum_{m|n} S_\ell(m) = \sum_{\ell m'|n} \sum_{r|m'} q^r \mu\left(\frac{m'}{r}\right) = q^{\frac{n}{\ell}},$$

and, if $\ell \nmid n$, then

$$\sum_{m|n} S_\ell(m) = 0.$$

Therefore,

$$\sum_{n=1}^{\infty} \frac{1}{n} \left( \sum_{m|n} \left( - \sum_{\ell=2}^{k} S_\ell(m) \right) \right) y^n$$

$$= - \sum_{\ell=2}^{k} \sum_{\substack{n=1 \\ \ell|n}}^{\infty} \frac{1}{n} q^{\frac{n}{\ell}} y^n = \sum_{\ell=2}^{k} \frac{1}{\ell} \log\,(1 - qy^\ell). \tag{8.15}$$

From (8.12), (8.13), (8.14), and (8.15) we obtain

$$Z(y) = \frac{1}{1-qy}(1-q_1 y) \prod_{s=k+1}^{\infty} \frac{1}{(1-qy^s)^{1/s}} e^{F(y)}.$$

This shows that $Z(y)$ is a meromorphic function in the disk $\left\{|y| < q^{-\frac{1}{k+1}}\right\}$, with a simple pole at $y = q^{-1}$ and a simple zero at $y = q_1^{-1} = q^{-1+\eta}$. It is easy to see that

$$G(n) = Aq^n + O\left(q^{\frac{n}{k+1}+\varepsilon n}\right)$$

with

$$A = \left(1 - q^{-\eta}\right) \prod_{s=k+1}^{\infty} \frac{1}{(1-q^{-s+1})^{\frac{1}{s}}} e^{F(q^{-1})} > 0.$$

We note that $\eta$ and $k$ can be chosen arbitrarily small and arbitrarily large independently. Therefore, this example shows that, no matter how small $\nu > 0$, in (8.11) is, $Z(y)$ may have a zero very close to $|y| = q^{-1}$.

This example also shows that the Riemann hypothesis can hold only for very special additive arithmetical semigroups.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

# CHAPTER 4

# MORE APPLICATIONS OF PRIME COUNTING

## 4.1 More Properties of Prime Divisor Functions in the "Classical" Case

We now return to the prime divisor functions $\omega$ and $\Omega$, in the "classical" case *when* $\mathcal{G}$ *satisfies Axiom* $\mathcal{A}^{\#}$*, and the generating function* $Z(y)$ *has no zeros for* $|y| \leq q^{-1}$ (i.e., there is no exceptional zero at $y = -q^{-1}$).

### 4.1.1 Some general results

For a start, consider the subsets $\mathcal{G}^{\Omega}_{\text{even}}$ and $\mathcal{G}^{\omega}_{\text{even}}$ of $\mathcal{G}$ consisting of all elements $a \in \mathcal{G}$ such that $\Omega(a)$ (respectively, $\omega(a)$) is *even*, and let $\mathcal{G}^{\Omega}_{\text{odd}}$ and $\mathcal{G}^{\omega}_{\text{odd}}$ denote the respective complements of these sets in $\mathcal{G}$. We wish to investigate the densities of these sets in $\mathcal{G}$, as well as their relative densities in the subset $\mathcal{G}_{(k)}$ of all $k$-free elements of $\mathcal{G}$ $(k \geq 2)$.

In order to explain the term "relative density" used here, let $E$ and $H$ denote subsets of $\mathcal{G}$, and let $\chi_E$ and $\chi_H$ denote their characteristic functions. Then the *total numbers* of elements of degree $N$ in $E$ and $H$ are $E(N) = \overline{\chi}_E(N)$, and $H(N) = \overline{\chi}_H(N)$, respectively. If the ratio $E(N)/H(N)$ tends

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

to a limit $\delta$ as $N \to \infty$, we call $\delta = \delta(E, H)$ the **relative asymptotic density** of $E$ in $H$. According to this definition (which is sufficiently general for present purposes), if $E$ has the relative density $\delta$ in $H$, then the ratio $E(N)/H(N)$ must be meaningful for all sufficiently large $N$, i.e., $H(N) > 0$ for all large enough $N$. Therefore a standard elementary theorem on limits implies further that

$$\delta = \lim_{N \to \infty} \left\{ \sum_{n \leq N} E(n) \right\} \bigg/ \left\{ \sum_{n \leq N} H(n) \right\} ;$$

thus the present terminology seems reasonable from an intuitive point of view, and is consistent with that for the "absolute" case $H = \mathcal{G}$ which was discussed in Section 1.3 earlier.

(4.1.1) THEOREM. *The sets $\mathcal{G}^{\Omega}_{\text{even}}$ and $\mathcal{G}^{\Omega}_{\text{odd}}$ both have asymptotic density $\frac{1}{2}$, as well as relative asymptotic density $\frac{1}{2}$ in the set $\mathcal{G}_{(k)}$ of all $k$-free elements of $\mathcal{G}$ $(k \geq 2)$. More precisely, for every $\alpha > 0$, as $N \to \infty$,*

$$\mathcal{G}^{\Omega}_{\text{even}}(N) = \frac{A}{2} q^N + O\left(N^{-\alpha} q^N\right) = \mathcal{G}^{\Omega}_{\text{odd}}(N),$$

$$\left(\mathcal{G}^{\Omega}_{\text{even}} \cap \mathcal{G}_{(k)}\right)(N) = \frac{A}{2} \left[Z(q^{-k})\right]^{-1} q^N + O\left(N^{-\alpha} q^N\right) = \left(\mathcal{G}^{\Omega}_{\text{odd}} \cap \mathcal{G}_{(k)}\right)(N).$$

PROOF. As with the corresponding Theorem 6.2.1 of [AB] subject to Axiom $\mathcal{A}$, our discussion of the distinction between the even and odd values of $\Omega$ is facilitated by consideration of the **Liouville** function $\lambda$ on $\mathcal{G}$ such that $\lambda(a) = (-1)^{\Omega(a)}$ for $a \in \mathcal{G}$, as well as the function $\lambda_k$ $(k \geq 2)$ such that $\lambda_k(a) = \lambda(a)$ if $a$ is $k$-free, while $\lambda_k(a) = 0$ otherwise. (Recall that $\lambda_2$ is simply the **Möbius** function $\mu$ on $\mathcal{G}$).

(4.1.2) LEMMA. *The functions $\lambda$, $\lambda_k$ (including $\mu$) have asymptotic mean-value zero.*

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

PROOF. By Theorem 3.3.1 of [AB], $\lambda^{\#}(y) = Z(y^2)/Z(y)$, while

$$\lambda_k^{\#}(y) = \begin{cases} Z(y^2)/Z(y)Z(y^k) & \text{if } k \text{ is even,} \\ \\ Z(y^2)Z(y^k)/Z(y)Z(y^{2k}) & \text{if } k \text{ is odd.} \end{cases}$$

These formulae, together with Proposition 1.2.1 and the non-existence of zeros of $Z(y)$ for $|y| \leq q^{-1}$, show that $\lambda^{\#}(y)$ and $\lambda_k^{\#}(y)$ are analytic functions of $y$ for $|y| \leq q^{-1}$. Therefore Lemma 2.2.3 implies that, for every $\alpha > 0$,

$$\overline{\lambda}(N) = O\left(N^{-\alpha}q^N\right) = \overline{\lambda}_k(N) \text{ as } N \to \infty. \qquad \square$$

In view of Lemma 4.1.2, Axiom $\mathcal{A}^{\#}$ and Proposition 1.5.7, the present theorem about $\Omega$ may now easily be deduced from the equations

$$\left.\begin{array}{c} \mathcal{G}^{\Omega}_{\text{even}}(N) + \mathcal{G}^{\Omega}_{\text{odd}}(N) = G(N) \\ \\ \mathcal{G}^{\Omega}_{\text{even}} - \mathcal{G}^{\Omega}_{\text{odd}}(N) = \overline{\lambda}(N) \end{array}\right\},$$

and

$$\left.\begin{array}{c} \left(\mathcal{G}^{\Omega}_{\text{even}} \cap \mathcal{G}_k\right)(N) + \left(\mathcal{G}^{\Omega}_{\text{even}} \cap \mathcal{G}_k\right)(N) = \mathcal{G}_k(N) \\ \left(\mathcal{G}^{\Omega}_{\text{even}} \cap \mathcal{G}_k\right)(N) - \left(\mathcal{G}^{\Omega}_{\text{even}} \cap \mathcal{G}_k\right)(N) = \overline{\lambda}_k(N) \end{array}\right\}. \qquad \square$$

The theorem corresponding to Theorem 3.9.1 for the function $\omega$ is:

(4.1.3) THEOREM. *The sets $\mathcal{G}^{\omega}_{\text{even}}$ and $\mathcal{G}^{\omega}_{\text{odd}}$ both have asymptotic density $\frac{1}{2}$, as well as relative asymptotic density $\frac{1}{2}$ in the set $\mathcal{G}_k$ of all $k$-free elements of $\mathcal{G}$ $(k \geq 2)$. More precisely, for every $\alpha > 0$, as $N \to \infty$,*

$$\mathcal{G}^{\omega}_{\text{even}}(N) = \frac{A}{2}q^N + O\left(N^{-\alpha}q^N\right) = \mathcal{G}^{\omega}_{\text{odd}}(N),$$

$$\left(\mathcal{G}^{\omega}_{\text{even}} \cap \mathcal{G}_k\right)(N) = \frac{A}{2}\left[Z(q^{-k})\right]^{-1}q^N + O\left(N^{-\alpha}q^N\right) = \left(\mathcal{G}^{\omega}_{\text{odd}} \cap \mathcal{G}_k\right)(N).$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

PROOF. For this theorem, we shall make use of the functions $\xi$ and $\xi_k$ analogous to $\lambda$ and $\lambda_k$, such that $\xi(a) = (-1)^{\omega(a)}$ for $a \in \mathcal{G}$, $\xi_k(a) = \xi(a)$ if $a$ is $k$–free, and $\xi_k(a) = 0$ otherwise. (Then $\xi_2$ also coincides with the Möbius function on $\mathcal{G}$.) Since $\omega$ is prime–independent and additive, $\xi$ and $\xi_k$ are *PIM*–functions, and so the Canonical Product Lemma 1.4.1 implies that (formally, at least)

$$\begin{cases} \xi^{\#}(y) = \prod\limits_{m>0} \left(1 - y^m - y^{2m} - \ldots - y^{rm} - \ldots\right)^{P(m)}, \\ \xi_k^{\#}(y) = \prod\limits_{m>0} \left(1 - y^m - y^{2m} - \ldots - y^{(k-1)m}\right)^{P(m)}. \end{cases} \tag{1.1}$$

Therefore

$$\begin{aligned} \xi^{\#}(y) &= \prod_{m>0} \left(1 - \frac{y^m}{1-y^m}\right)^{P(m)} \\ &= \frac{1}{Z_G(y)} \prod_{m>0} \left\{(1-y^m)^{-1}\left(1 - \frac{y^m}{1-y^m}\right)\right\}^{P(m)} \\ &= \mu^{\#}(y) \prod_{m>0} \left\{1 - \frac{y^{2m}}{(1-y^m)^2}\right\}^{P(m)}. \end{aligned}$$

Now, by Proposition 1.2.1 and $Z(y) \neq 0$ for $|y| \leq q^{-1}$, $\mu^{\#}(y)$ is analytic for $|y| \leq q^{-1}$ and (in the ordinary analytical sense) is represented by the absolutely convergent product $\prod_{m>0} (1-y^n)^{P(m)}$ when $|y| < q^{-1}$. In particular, this implies that $\sum_{m>0} P(m)y^{2m}$ is absolutely convergent for $|y| < q^{-\frac{1}{2}}$, and so

$$\sum_{m>0} P(m) \frac{y^{2m}}{(1-y^m)^2}$$

is also absolutely convergent for such $y$. Therefore the second product in the last expression for $\xi^{\#}(y)$ above is absolutely convergent when $|y| < q^{-\frac{1}{2}}$, and so $\xi^{\#}(y)$ is an analytic function of $y$ in the closed disc $|y| \leq q^{-1}$.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Next, in a similar way, note that

$$\xi_k^{\#}(y) = \prod_{m>0} \left(1 + \frac{y^{km} - y^m}{1 - y^m}\right)^{P(m)} = \mu^{\#}(y) \prod_{m>0} \left(1 + \frac{y^{km} - y^{2m}}{(1 - y^m)^2}\right)^{P(m)}.$$

Since $|y^{km} - y^{2m}| = |y^{(k-2)m} - 1|\,|y^{2m}| < 2|y^{2m}|$ for $|y| < 1$, it follows from the discussion above that the second product in the last expression for $\xi_k^{\#}(y)$ is also absolutely convergent when $|y| < q^{-\frac{1}{2}}$. Thus $\xi_k^{\#}(y)$ is also analytic for $|y| \leq q^{-1}$.

By Lemma 2.2.3, the above conclusions imply that, for any $\alpha > 0$

$$\overline{\xi}(N) = O\left(N^{-\alpha} q^N\right) = \overline{\xi}_k(N) \text{ as } N \to \infty.$$

The proof of Theorem 4.1.3 may then be completed by an argument directly analogous to that which concluded the proof of Theorem 4.1.1. □

Another approach to the "statistical" properties of functions like $\Omega$ and $\omega$ is to consider the frequency with which they take on some *particular* value $k \geq 1$. For this purpose, let $\tau_k(N)$, $\rho_k(N)$ and $\pi_k(N)$ denote the total numbers of elements $a \in \mathcal{G}$ of degree $N$ such that (i) $\Omega(a) = k$, or (ii) $\omega(a) = k$, or (iii) $\omega(a) = k$ and $a$ is square–free, respectively. For $\tau_k(N)$ and $\pi_k(N)$, the following theorem was proved by S.D. Cohen [2] in the case when $\mathcal{G}$ is the special semigroup $\mathcal{G}_q$.

(4.1.4) THEOREM. *As $N \to \infty$, each of the functions $\tau_k(N)$, $\rho_k(N)$ and $\pi_k(N)$ has the asymptotic value*

$$\frac{(\log N)^{k-1}}{(k-1)!N} q^N + O\left(\frac{(\log N)^{k-2}}{N} q^N\right).$$

PROOF. The functions $\tau_1(N)$, $\pi_1(N)$ coincide with $P(N)$, and so the stated conclusions about $\tau_1$ and $\pi_1$ are immediate consequences of the abstract prime number theorem (3.4.5). Now suppose that $k > 1$, and (for $r \geq 1$) consider the additional function

$$V_r(N) = \sum_{\partial(p_1 p_2 \cdots p_r)=N} 1,$$

where the sum is over all ordered $r$–tuples $(p_1, \ldots, p_r)$ of primes $p_i$ with $\partial(p_1 p_2 \ldots p_r) = N$. Then

$$r!\pi_r(N) \leq V_r(N) \leq r!\tau_r(N),$$

and

$$\begin{aligned} \tau_k(N) - \pi_k(N) &\leq \sum_{\partial(p_1^2 p_2 \cdots p_{k-1})=N} 1 \\ &= \sum_{2\partial(p_1)\leq N} \; \sum_{\partial(p_2 p_3 \cdots p_{k-1})=N-2\partial(p_1)} 1 \\ &\leq \sum_{m \leq \frac{1}{2}N} P(m) V_{k-2}(N-2m), \end{aligned}$$

where $V_0(N) = 1$. Therefore we obtain:

$$\frac{1}{k!} V_k(N) \leq \tau_k(N) \leq \pi_k(N) + \sum_{m \leq \frac{1}{2}N} P(m) V_{k-2}(N-2m), \tag{1.2}$$

and

$$\frac{1}{k!} V_k(N) - \sum_{m \leq \frac{1}{2}N} P(m) V_{k-2}(N-2m) \leq \pi_k(N) \leq \frac{1}{k!} V_k(N). \tag{1.3}$$

Now consider:

(4.1.5) LEMMA. *As $N \to \infty$,*

$$V_k(N) = \frac{k}{N} (\log N)^{k-1} q^N + O\left(\frac{(\log N)^{k-2}}{N} q^N\right).$$

PROOF. By the abstract prime number theorem (3.4.5), the stated formula is certainly valid for $V_1(N) = P(N)$. Now, as an inductive hypothesis on $k$, assume the formula for $V_k$, and consider

$$\begin{aligned}
kNV_{k+1}(N) &= \sum_{\partial(p_1p_2\dots p_{k+1})=N} k\partial(p_1p_2\dots p_{k+1}) \\
&= \sum_{\partial(p_1p_2\dots p_{k+1})=N} \Big\{\partial(p_2p_3\dots p_{k+1}) + \partial(p_1p_3\dots p_{k+1}) + \\
&\qquad + \dots + \partial(p_1p_2\dots p_k)\Big\} \\
&= (k+1)\sum_{\partial(p_1)\leq N}\ \sum_{\partial(p_2p_3\dots p_{k+1})=N-\partial(p_1)} \partial(p_2p_3\dots p_{k+1}) \\
&= (k+1)\sum_{\partial(p_1)\leq N} [N-\partial(p_1)]\, V_k\left(N-\partial(p_1)\right) \\
&= (k+1)\sum_{m\leq N-1}(N-m)P(m)V_k(N-m).
\end{aligned}$$

Therefore, by the assumption on $V_k$,

$$\begin{aligned}
&kNV_{k+1}(N) \\
&= (k+1)\sum_{m\leq N-1}(N-m)\left[\frac{q^m}{m} + O\left(\frac{q^m}{m}\right)\right] \\
&\quad \times \frac{k}{N-m}\Big[\big(\log(N-m)\big)^{k-1}q^{N-m} + O\Big(\big(\log(N-m)\big)^{k-2}q^{N-m}\Big)\Big] \\
&= k(k+1)q^N \sum_{m\leq N-1}\left\{\frac{1}{m}\big(\log(N-m)\big)^{k-1} + O\left(\frac{1}{m}(\log N)^{k-2}\right)\right\} \\
&= k(k+1)q^N\left[(\log N)^k + O((\log N)^{k-1})\right],
\end{aligned}$$

by Lemma 4.1.6 below. Hence the stated asymptotic formula for $V_k(N)$ follows by induction on $k$. □

4.1.6 LEMMA. *For any positive integer $k$, as $N \to \infty$,*

$$\sum_{m\leq N-1}\frac{1}{m}\big(\log(N-m)\big)^{k-1} = (\log N)^k + O((\log N)^{k-1}).$$

PROOF. We have

$$\begin{aligned}\sum_{m\le N-1}\frac{1}{m}(\log(N-m))^{k-1} &= \sum_{m\le N-1}\frac{1}{N-m}(\log m)^{k-1}\\ &= \frac{1}{N}\sum_{m\le N-1}\left(1+\frac{m}{N}+\frac{m^2}{N^2}+\dots\right)(\log m)^{k-1}.\end{aligned}$$

Now, for any $r\ge 0$ and $k>1$, partial summation gives

$$\begin{aligned}\sum_{m\le N} m^r(\log m)^k &= (\log N)^k\sum_{m\le N} m^r - k\int_1^N t^{-1}(\log t)^{k-1}\left(\sum_{m\le t} m^r\right)dt\\ &= \left[\frac{N^{r+1}}{r+1}+O(N^r)\right](\log N)^k + O\left(\int_1^N(\log t)^{k-1}t^r dt\right)\end{aligned}$$

by the formula

$$\sum_{m\le x} m^r = \frac{x^{r+1}}{r+1}+O(x^r).$$

Therefore

$$\begin{aligned}\sum_{m\le N} m^r(\log m)^k &= \left[\frac{N^{r+1}}{r+1}+O(N^r)\right](\log N)^k + O\left((\log N)^{k-1}\int_1^N t^r dt\right)\\ &= \frac{N^{r+1}}{r+1}(\log N)^k + O\left(N^{r+1}(\log N)^{k-1}\right).\end{aligned}$$

It now follows that, for $k\ge 2$,

$$\begin{aligned}&\sum_{m\le N-1}\frac{1}{m}(\log(N-m))^{k-1}\\ &=\sum_{r=0}^{\infty}\frac{1}{N^{r+1}}\sum_{m\le N-1} m^r(\log m)^{k-1}\\ &=\sum_{r=0}^{\infty}\frac{1}{r+1}\left(1-\frac{1}{N}\right)^{r+1}\left[(\log N)^{k-1}+O((\log N)^{k-2})\right]\\ &=\left[(\log N)^{k-1}+O((\log N)^{k-2})\right]\log\left\{1-\left(1-\frac{1}{N}\right)\right\}^{-1}\\ &=(\log N)^k+O((\log N)^{k-1}).\qquad\square\end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

The assertions of Theorem 4.1.4 about $\tau_k(N)$ and $\pi_k(N)$ may now be deduced from the inequalities (1.2) and (1.3) above, together with the following consequences of Lemma 4.1.5 and the following lemma, which is easily deduced by partial summation:

(4.1.7) LEMMA. *For any real $\alpha$, and $q > 1$,*

$$\sum_{r \leq n} r^\alpha q^r = \frac{1}{q-1} n^\alpha q^{n+1} + O\left(n^{\alpha-1} q^n\right) \quad \text{as } n \to \infty. \qquad \square$$

Now consider two cases:

*Case (i).* For $k = 2$,

$$\sum_{m \leq \frac{1}{2}N} P(m) V_{k-2}(N-2m) = O\left(\sum_{m \leq \frac{1}{2}N} \frac{q^m}{m}\right) = O\left(N^{-1} q^{\frac{1}{2}N}\right).$$

*Case (ii).* For $k > 2$,

$$\begin{aligned}
&\sum_{m \leq \frac{1}{2}N} P(m) V_{k-2}(N-2m) \\
&\quad = O\left(\sum_{m < \frac{1}{2}N} \frac{q^m}{m} \frac{(\log(N-2m))^{k-3}}{N-2m} q^{N-2m}\right) \\
&\quad = O\left((\log N)^{k-3} q^N \sum_{m < \frac{1}{2}N} \left(\frac{1}{m} + \frac{2}{N-2m}\right) \frac{q^{-m}}{N}\right) \\
&\quad = O\left((\log N)^{k-3} N^{-1} q^N \sum_{m < \frac{1}{2}N} q^{-m}\right) \\
&\quad = O\left((\log N)^{k-3} N^{-1} q^N\right).
\end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

In order to complete the proof of Theorem 4.1.4, it remains to consider the function $\rho_k(N)$: By definition of $\rho_k(N)$ and $\pi_k(N)$, $\rho_k(N) - \pi_k(N)$ is equal to the total number of elements $a \in \mathcal{G}$ of degree $N$ that can be expressed in the form $a = p^m b$ for some $p \in \mathcal{P}$, $m \geq 2$, and an element $b$ with $\omega(b) = k-1$. Thus

$$\begin{aligned}
0 \leq \rho_k(N) - \pi_k(N) &= \sum_{\substack{\omega(b)=k-1,\\ \partial(b)\leq N-2}} \sum_{2\leq m\leq N-\partial(b)} \sum_{\partial(p)=\frac{N-\partial(b)}{m}} 1 \\
&= \sum_{\substack{\omega(b)=k-1,\\ \partial(b)\leq N-2}} \sum_{2\leq m\leq N-\partial(b)} O\left(\frac{m}{N-\partial(b)} q^{\frac{N-\partial(b)}{m}}\right) \\
&= O\left(\sum_{\substack{\omega(b)=k-1,\\ \partial(b)\leq N-2}} q^{\frac{1}{2}[N-\partial(b)]}\right).
\end{aligned}$$

Therefore

$$0 \leq \rho_k(N) - \pi_k(N) = O\left(q^{\frac{1}{2}N} \sum_{r\leq N-2} q^{-\frac{1}{2}r} \rho_{k-1}(r)\right).$$

Now note that $\rho_1(N)$ is the number of prime-powers $p^m \in \mathcal{G}$ of degree $N$, and hence that

$$\begin{aligned}
\rho_1(N) &= \sum_{m\leq N} \sum_{\partial(p)=\frac{N}{m}} 1 = P(N) + \sum_{2\leq m\leq N} O\left(q^{N/m}\right) \\
&= P(N) + O\left(Nq^{\frac{1}{2}N}\right) = \frac{q^N}{N} + O\left(N^{-\alpha} q^N\right),
\end{aligned}$$

for any $\alpha > 1$. Thus the assertion of Theorem 4.1.4 holds for $\rho_1(N)$. Then assume the corresponding conclusion for $\rho_{k-1}(N)$, $k \geq 2$. In that case,

$$\sum_{r\leq N} q^{-\frac{1}{2}r} \rho_{k-1}(r) = O\left(\sum_{r\leq N} \frac{(\log r)^{k-2}}{r} q^{\frac{1}{2}r}\right)$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

$$
\begin{aligned}
&= O\left((\log N)^{k-2} \sum_{r \leq N} \frac{1}{r} q^{\frac{1}{2}r}\right) \\
&= O\left((\log N)^{k-2} \frac{1}{N} q^{\frac{1}{2}N}\right),
\end{aligned}
$$

by Lemma 4.1.7. Therefore the above inequality for $\rho_k(N) - \pi_k(N)$ together with the result for $\pi_k(N)$ already proved leads to the required conclusion about $\rho_k(N)$. Hence the stated conclusion follows by induction on $k$. □

### 4.1.2 Sharper estimates in concrete cases

The error estimates $O\left(N^{-\alpha} q^N\right)$ in Theorems 4.1.1 and 4.1.3 may be sharpened as below in various concrete cases:

(4.1.8) Lemma. *Let $\mathcal{G}$ denote any additive arithmetical semigroup with the properties specified in Lemma 3.1.4, and let $\mu$, $\lambda$, $\lambda_k$, $\xi$ and $\xi_k$ denote the corresponding arithmetical functions on $\mathcal{G}$. Then as $N \to \infty$*

$$
\overline{\mu}(N) = O\left(N^{M-1} q^{\theta N}\right), \quad \overline{\lambda}(N) = O\left(N^{M} q^{\theta N}\right), \quad \overline{\lambda}_k(N) = O\left(N^{2M-1} q^{\theta N}\right),
$$

$$
\overline{\xi}(N) = O\left(N^{M-1} q^{\theta N}\right) = \overline{\xi}_k(N),
$$

*where $\theta$ is the number defined in Lemma 3.1.4.*

Proof. Firstly, in the notation of Lemma 1.4.2, we have

$$
\begin{aligned}
\mu^{\#}(y) &= \frac{1}{Z(y)} = (1 - qy) \prod_{i=1}^{M} (1 - \alpha_i y)^{-1} \\
&= 1 + \sum_{n=1}^{\infty} \left(c_n - q c_{n-1}\right) y^n,
\end{aligned}
$$

where

$$c_n = \sum_{k_1+\ldots+k_M=n} \alpha_1^{k_1}\alpha_2^{k_2}\ldots\alpha_M^{k_M}.$$

Since $|\alpha_i| \leq q^\theta$ (by definition of $\theta$), it follows that

$$|c_n| \leq \binom{-M}{n}(\,-\,q^\theta)^n = \binom{M+n-1}{n} q^{\theta n} \sim \frac{n^{M-1}}{(M-1)!}\, q^{\theta n} \text{ as } n \to \infty.$$

Hence

$$\overline{\mu}(N) = c_N - q c_{N-1} = O\left(N^{M-1} q^{\theta N}\right) \text{ as } N \to \infty.$$

Next, the preceding conclusion and the equation $\lambda^{\#}(y) = Z(y^2)\mu^{\#}(y)$ imply that

$$\overline{\lambda}(N) = \sum_{0 \leq r \leq \frac{1}{2}N} H^{\#}(r)\overline{\mu}(N-2r) = O\left(\sum_{0 \leq r \leq \frac{1}{2}N} q^r N^{M-1} q^{\theta(N-2r)}\right),$$

since a discussion parallel to that of Example 1.1.5 earlier shows easily that the total number $G(n)$ of elements of degree $n$ in $\mathcal{G}$ satisfies:

$$G(n) = Aq^n + O(1) \text{ as } n \to \infty,$$

where $A = Q(q^{-1})$. Since $\theta \geq \frac{1}{2}$, it then follows that

$$\overline{\lambda}(N) = O\left(N^{M-1} q^{\theta N} \sum_{r \leq \frac{1}{2}N} q^{(1-2\theta)r}\right) = O\left(N^M q^{\theta N}\right).$$

Now, for an *even* integer $k$, the conclusions already derived, together with the equation $\lambda_k^{\#}(y) = \lambda^{\#}(y)\mu^{\#}(y^k)$, lead to:

$$\begin{aligned} \overline{\lambda}_k(N) &= \sum_{0 \leq r \leq N/k} \overline{\lambda}(N-kr)\overline{\mu}(r) = O\left(\sum_{r \leq N/k} N^M q^{\theta(N-kr)} N^{M-1} q^{\theta r}\right) \\ &= O\left(N^{2M-1} q^{\theta N} \sum_{r \leq N/k} q^{\theta(1-k)r}\right) = O\left(N^{2M-1} q^{\theta N}\right). \end{aligned}$$

Then, for an *odd* integer $k$, the equation $\lambda_k^{\#}(y) = Z(y^k)\lambda_{2k}^{\#}(y)$, together with the preceding result for $\lambda_{2k}$, yields:

$$\begin{aligned}\overline{\lambda}_k(N) &= \sum_{0\leq r\leq N/k} H^{\#}(r)\overline{\lambda}_{2k}(N-kr) = O\left(\sum_{r\leq N/k} q^r N^{2M-1} q^{\theta(N-kr)}\right) \\ &= O\left(N^{2M-1}q^{\theta N}\sum_{r\leq N/k} q^{(1-k\theta)r}\right) = O\left(N^{2M-1}q^{\theta N}\right),\end{aligned}$$

since $\theta > 1/k$.

Lastly consider the functions $\xi$ and $\xi_k$ on $\mathcal{G}$, corresponding to those discussed in the proof of Theorem 3.9.3. Regarding $\xi$, the proof of Theorem 4.1.3 implies that $\xi^{\#}(y) = \mu^{\#}(y)F(y)$ where $F(y)$ is an analytic function of $y$ for $|y| < q^{-\frac{1}{2}}$. Hence, if $F(y) = \sum_{n=0}^{\infty} a_n y^n$,

$$\begin{aligned}\overline{\xi}(N) &= \sum_{0\leq r\leq N} \overline{\mu}(N-r)a_r = O\left(\sum_{r\leq N} N^{M-1}q^{\theta(N-r)}|a_r|\right) \\ &= O\left(N^{M-1}q^{\theta N}\sum_{r\leq N} |a_r|q^{-\theta r}\right).\end{aligned}$$

This conclusion implies the stated estimate for $\overline{\xi}(N)$, if $\theta > \frac{1}{2}$. On the other hand, if $\theta = \frac{1}{2}$, it follows from the formula for $\mu^{\#}(y)$ stated at the beginning of this proof that $\mu^{\#}(y)$ is an analytic function of $y$ for $|y| < q^{-\frac{1}{2}}$; therefore the earlier reasoning (in the proof of Theorem 4.1.3) about the function $F(y)$ now implies that it is analytic for $|y| < q^{-\frac{1}{4}}$. Thus the stated estimate for $\overline{\xi}(N)$ also follows when $\theta = \frac{1}{2}$. The discussion of $\overline{\xi}_k(N)$ is similar. □

For the semigroups $\mathcal{G}_K$ and $\mathcal{G}_D$ of Examples 1.1.4–5, Lemma 4.1.8 leads to:

(4.1.9) THEOREM. *For both the special arithmetical semigroups $\mathcal{G}_K$*

*and $\mathcal{G}_D$, there exists a constant $M$ such that, as $N \to \infty$,*

$$\overline{\mu}(N) = O\left(N^{M-1}q^{\frac{1}{2}N}\right), \quad \overline{\lambda}(N) = O\left(N^{M}q^{\frac{1}{2}N}\right), \quad \overline{\lambda}_k(N) = O\left(N^{2M-1}q^{\frac{1}{2}N}\right),$$

*and*

$$\overline{\xi}(N) = O\left(N^{M-1}q^{\frac{1}{2}N}\right) = \overline{\xi}_k(N).$$

PROOF. By the earlier discussion of the zeta function of $\mathcal{G}_D$, this semigroup satisfies the hypotheses on $\mathcal{G}$ in Lemma 4.1.8, with $\theta = \frac{1}{2}$. Hence the case of $\mathcal{G}_D$ follows immediately, with $M$ equal to the degree of the polynomial $(1 - qy)Z(y)$.

For $\mathcal{G}_K$, we have the generating function

$$Z_K(y) = \frac{L(y)}{(1-y)(1-qy)},$$

where $L(y)$ is a polynomial of degree $2g$ in $y$, $g$ being the "genus" of $K$ (see Example 1.1.4). In addition,

$$L(y) = \prod_{i=1}^{2g}(1 - \alpha_i y),$$

where $|\alpha_i| = q^{\frac{1}{2}}$. Therefore, for the semigroup $\mathcal{G}_K$,

$$\begin{aligned} \mu^{\#}(y) &= (1-y)(1-qy)\prod_{i=1}^{2g}(1-\alpha_i y)^{-1} \\ &= 1 + \sum_{n=1}^{\infty}(\mu_n - \mu_{n-1})y^n, \end{aligned}$$

where

$$\sum_{n=0}^{\infty}\mu_n y^n = (1-qy)\prod_{i=1}^{2g}(1-\alpha_i y)^{-1}.$$

Then, exactly as in the first part of the proof of Lemma 4.1.8, it can be verified that $\mu_N = O\left(N^{M-1}q^{\frac{1}{2}N}\right)$, and hence that

$$\overline{\mu}(N) = O\left(N^{M-1}q^{\frac{1}{2}N}\right),$$

where $M = 2g$. The remaining estimates may now be deduced from this one by essentially the same arguments as those used in the latter part of the proof of Lemma 4.1.8, when $\theta = \frac{1}{2}$. □

The particularly sharp information about the generating functions $Z_D(y)$ and $Z_K(y)$ can be used to refine various other estimates concerning arithmetical functions on $\mathcal{G}_D$ and $\mathcal{G}_K$; for example this is true for many of the estimates discussed in Chapters 1, 2. However, similar refinements seem to be less easy to derive for functions on the associated arithmetical semigroups of the categories $\mathcal{F} = \mathcal{F}_D$ and $\mathcal{S} = \mathcal{S}_D$, and so the abstract theory of semigroups satisfying Axiom $\mathcal{A}^{\#}$ is especially convenient for the purpose of deriving asymptotic conclusions about *those* specific systems. Further, in many cases, the consequences of the abstract theory are probably also sufficient for the needs of particular applications to $\mathcal{G}_D$ and $\mathcal{G}_K$. For these reasons, it seems usually to be more profitable to study consequences of Axiom $\mathcal{A}^{\#}$ (and if necessary the assumption that $Z(y) \neq 0$ for $|y| \leq q^{-1}$) than to undertake specific corresponding investigations of our special examples of arithmetical semigroups satisfying such conditions. (As with all axiomatic studies of course, this procedure also has the advantage of admitting the possibility of interesting applications to further concrete systems not yet treated in such a context.) Consequently, we shall not pursue the search for sharper estimates further over here, apart from including the following slightly weaker form of Theorem 3.1.9 within the context of the categories $\mathcal{F}$ and $\mathcal{S}$:

(4.1.10) THEOREM. *For the associated arithmetical semigroups of the categories $\mathcal{F} = \mathcal{F}_D$ and $\mathcal{S} = \mathcal{S}_D$, the quantities $\overline{\mu}(N)$, $\overline{\lambda}(N)$, $\overline{\lambda}_k(N)$, $\overline{\xi}(N)$*

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

*and* $\overline{\xi}_k(N)$ *are of the form*

$$O_\varepsilon\left(q^{\frac{1}{2}N}(1+\varepsilon)^N\right) \quad \textit{as } N \to \infty,$$

*where* $\varepsilon > 0$ *is arbitrary (but the implied constant may depend on* $\varepsilon$*).*

PROOF. Let $\mu_D$, $\mu_{\mathcal{F}}$ and $\mu_{\mathcal{S}}$ denote the Möbius functions relative to the semigroups $\mathcal{G}_D$, $\mathcal{G}_{\mathcal{F}}$ and $\mathcal{G}_{\mathcal{S}}$ corresponding to $D$, $\mathcal{F}$ and $\mathcal{S}$, respectively. By the proof of Theorem 2.1.5, when $|y| < q^{-1}$,

$$Z_{\mathcal{F}}(y) = Z_D(y)F_2(y),$$

where $F_2(y)$ is a non-zero analytic function of $y$ for $|y| < q^{-\frac{1}{2}}$. Since (by the proof of Lemma 4.1.8) $\mu_D^{\#}(y)$ is an analytic function of $y$ for $|y| < q^{-\frac{1}{2}}$, it follows that $\mu_{\mathcal{F}}^{\#}(y)$ is analytic for $|y| < q^{-\frac{1}{2}}$. By the standard formula for the radius of convergence of a power series, this implies that

$$\limsup_{N\to\infty} |\overline{\mu}_{\mathcal{F}}(N)|^{1/N} \le q^{\frac{1}{2}}.$$

Hence (for any $\varepsilon > 0$)

$$\overline{\mu}_{\mathcal{F}}(N) = O\left(q^{\frac{1}{2}N}(1+\varepsilon)^N\right) \text{ as } N \to \infty.$$

Now consider the Liouville and other functions $\lambda$, $\lambda_k$, $\xi$ and $\xi_k$ relative to $\mathcal{G}_{\mathcal{F}}$. Following the general line of proof of Lemma 4.1.8, now choose any fixed $\varepsilon > 0$, and note that the equation $\lambda^{\#}(y) = Z_{\mathcal{F}}(y^2)\mu_{\mathcal{F}}^{\#}(y)$ then implies that

$$\begin{aligned}
\overline{\lambda}(N) &= \sum_{0\le r\le \frac{1}{2}N} G_{\mathcal{F}}(r)\overline{\mu}_{\mathcal{F}}(N-2r) \\
&= O\left(\sum_{r\le\frac{1}{2}N} q^r q^{\frac{1}{2}(N-2r)}(1+\varepsilon)^{N-2r}\right) \\
&= O\left(q^{\frac{1}{2}N}(1+\varepsilon)^N \sum_{r\le\frac{1}{2}N}(1+\varepsilon)^{-2r}\right) \\
&= O\left(q^{\frac{1}{2}N}(1+\varepsilon)^N\right).
\end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Next, for an *even* integer $k$, we see that the equation $\lambda_k^{\#}(y) = \lambda^{\#}(y)\mu_{\mathcal{F}}^{\#}(y^k)$ leads to

$$\begin{aligned}
\overline{\lambda}_k(N) &= \sum_{0\leq r\leq N/k} \overline{\lambda}(N-kr)\overline{\mu}_{\mathcal{F}}(r) \\
&= O\left(\sum_{r\leq N/K} q^{\frac{1}{2}(N-kr)}(1+\varepsilon)^{N-kr}q^{\frac{1}{2}r}(1+\varepsilon)^{r}\right) \\
&= O\left(q^{\frac{1}{2}N}(1+\varepsilon)^{N}\sum_{r\leq N/k} q^{\frac{1}{2}(1-k)r}(1+\varepsilon)^{(1-k)r}\right) \\
&= O\left(q^{\frac{1}{2}N}(1+\varepsilon)^{N}\right).
\end{aligned}$$

The case of $\lambda_k$ when $k$ is *odd* will be left as an exercise.

Now consider the function $\xi$. Since $\mu_{\mathcal{F}}^{\#}(y)$ is analytic for $|y| < q^{-\frac{1}{2}}$, the function $F(y)$ such that $\xi^{\#}(y) = \mu_{\mathcal{F}}^{\#}(y)F(y)$ again turns out to be analytic for $|y| < q^{-\frac{1}{4}}$. Therefore, if $F(y) = \sum_{n=0}^{\infty} a_n y^n$,

$$\begin{aligned}
\overline{\xi}(N) &= \sum_{0\leq r\leq N} \overline{\mu}_{\mathcal{F}}(N-r)a_r = O\left(\sum_{r\leq N} q^{\frac{1}{2}(N-r)}(1+\varepsilon)^{N-r}|a_r|\right) \\
&= O\left(q^{\frac{1}{2}N}(1+\varepsilon)^{N}\sum_{r\leq N}|a_r|q^{-\frac{1}{2}r}(1+\varepsilon)^{-r}\right) = O\left(q^{\frac{1}{2}N}(1+\varepsilon)^{N}\right).
\end{aligned}$$

Finally, the cases of $\xi_k$ and of the functions on the semigroups $\mathcal{G}_{\mathcal{S}}$ will also be left as exercises. □

## 4.2 Maximum Orders of Magnitude in the "Classical Case"

In addition to studying the average values or closely related "statistical" properties of arithmetical functions, it is sometimes interesting to investigate the "extreme" values of such functions in the sense of their (suitably interpreted) *maximum* and *minimum* orders of magnitude. For unbounded special functions of the kinds considered earlier, one approach to a definition of the last two terms is as follows (cf. also [AB], Chapter 5, §2). In this section, *we shall again assume* Axiom $\mathcal{A}^{\#}$ *and* $Z(y) \neq 0$ for $|y| \leq q^{-1}$.

Given any non-negative real-valued arithmetical function $f$ on $\mathcal{G}$, and a positive real-valued function $F$ (defined for all sufficiently large real numbers), the values $f(a)$ $[a \in \mathcal{G}]$ are said to have the **maximum order of magnitude** $F(|a|)$ for $|a|$ large provided that

$$\limsup_{|a|\to\infty} \frac{f(a)}{F(|a|)} = 1.$$

If (instead)

$$\liminf_{|a|\to\infty} \frac{f(a)}{F(|a|)} = 1$$

then the values $f(a)$ are said to have the **minimum** order of magnitude $F(|a|)$. Although these definitions are slightly restrictive, they were adequate for the particular functions studied in [AB]; in the present situation, apart from perhaps wishing to re-phrase the above definitions in terms of the degree function $\partial$, one might also like to investigate properties of the associated ordinary arithmetical functions

$$f_{\max}(N) = \max_{\partial(a)=N} f(a), \text{ and } f_{\min}(N) = \min_{\partial(a)=N} f(a).$$

(For example, if $\mathcal{G}$ contains a prime of degree 1, it is not hard to verify that $\omega_{\min}(N) = 1$, $d_{*\min}(N) = 2$, and $\Omega_{\max}(N) = N$ for every positive integer $N$.)

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

In general there are many unsolved questions regarding the determination of maximum and minimum orders of magnitude for a given arithmetical function $f$, and the same is true for the related functions $f_{\max}(N)$ and $f_{\min}(N)$. Consequently, this section contains only a few and fairly restricted results, concerning maxima in particular.

One moderately general theorem, which yields partial information about maximum orders of magnitude, appears under the heading of Corollary 5.2.8 in [AB]. A special case of this, which is adequate for present purposes, may be formulated as follows:

(4.2.1) THEOREM. *Let $\mathcal{H}$ denote any arithmetical semigroup such that*

$$N_H(x) = \sum_{n\leq x} H(n) = O(x^\delta) \textit{ as } x \to \infty, \textit{ and } \theta_H(x) > Cx^\delta,$$

*where $\delta$, $C$ are positive constants, and*

$$\theta_H(x) = \sum_{\text{prime } p,\, |p|\leq x} \log|p|.$$

*Let $f$ denote a non-negative real-valued multiplicative function on $\mathcal{H}$ such that*

*(i) for some constant $B > 0$, $f(p^r) \leq e^{B\sqrt{r}}$ for all prime-powers $p^r \neq 1$,*

*(ii) for some integer $t \geq 1$, there is a constant $\tau \geq 1$ with $\tau = [f(p^t)]^{\delta/t} \geq [f(p^r)]^{\delta/r}$ for all prime-powers $p^r \neq 1$.*

*Under these circumstances,* $\log f(a)$ *has the maximum order of magnitude*

$$\frac{(\log\tau)(\log|a|)}{\log\log|a|} \textit{ for } |a| \textit{ large.} \qquad \square$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

For our semigroup $\mathcal{G}$ satisfying Axiom $\mathcal{A}^{\#}$ without $Z(y) = 0$ for $|y| \leq q^{-1}$, this theorem implies:

(4.2.2) COROLLARY. *Let $f$ denote a non-negative real-valued multiplicative function on $\mathcal{G}$ such that:*

*(i) for some constant $B > 0$, $f(p^r) \leq e^{B\sqrt{r}}$ for all prime-powers $p^r \neq 1$,*

*(ii) for some integer $t \geq 1$, there is a constant $\tau \geq 1$ with $\tau = [f(p^t)]^{1/t} \geq [f(p^r)]^{1/r}$ for all prime-powers $p^r \neq 1$.*

*Then* $\log f(a)$ *has the maximum order of magnitude*

$$\frac{(\log \tau)(\log |a|)}{\log\log |a|},$$

*and hence*

$$\limsup_{N\to\infty} \frac{\log N}{N \log q} \log f_{\max}(N) = \log \tau.$$

PROOF. If $\mathcal{G}$ is regarded as an arithmetical semigroup relative to the norm $|a| = q^{\partial(a)}$, it follows from remarks made at the end of Section 1.1, that $N_G(x) = O(x)$ as $x \to \infty$. Also, in the present case,

$$\begin{aligned} \theta_G(x) &= \sum_{p\in\mathcal{P},\, q^{\partial(p)}\leq x} \partial(p) \log q = \sum_{r \leq \frac{\log x}{\log q}} rP(r) \log q \\ &= (\log q) \sum_{r\leq N} \left\{ q^r + O\left(r^{-\alpha} q^r\right)\right\}, \end{aligned}$$

where $N = \left[\frac{\log x}{\log q}\right]$, and $\alpha > 0$ is arbitrary. Therefore, by Lemma 3.9.7,

$$\begin{aligned} \theta_G(x) &= (\log q) \left\{ \frac{q}{q-1} \left(q^N - 1\right) + O\left(N^{-\alpha} q^N\right)\right\} > Cq^N \\ &> Cq^{\left(\frac{\log x}{\log q} - 1\right)} = \frac{C}{q} x, \end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

for some positive constant $C$. This shows that Theorem 4.2.1 (with $\delta = 1$) is applicable here, and yields the assertion about the maximum order of magnitude of $\log f(a)$.

In order to deduce the final conclusion of the corollary in detail, note that the above conclusion about the maximum order of magnitude of $\log f(a)$ implies that (for any $\varepsilon > 0$)

$$\log f(a) < \frac{(\log \tau)(\log |a|)}{\log\log |a|}(1+\varepsilon)$$

whenever $|a|$ is sufficiently large, while

$$\log f(a) > \frac{(\log \tau)(\log |a|)}{\log\log |a|}(1-\varepsilon)$$

for infinitely many $a \in \mathcal{G}$. Therefore, whenever $N$ is sufficiently large, there exist elements $a_N \in \mathcal{G}$ of degree $N$ such that

$$\begin{aligned}\log f_{\max}(N) &= \log f(a_N) < \frac{(\log \tau)N\log q}{\log N + \log\log q}(1+\varepsilon) \\ &< \frac{(\log \tau)N\log q}{\log N}(1+\varepsilon'),\end{aligned}$$

for arbitrary $\varepsilon' > 0$ when $N$ is sufficiently large. On the other hand, for infinitely many integers $N$ there are corresponding elements $b_N \in \mathcal{G}$ of degree $N$ such that

$$\begin{aligned}\log f_{\max}(N) &\geq \log f(b_N) > \frac{(\log \tau)N\log q}{\log N + \log\log q}(1-\varepsilon) \\ &> \frac{(\log \tau)N\log q}{\log N}(1-\varepsilon'),\end{aligned}$$

for arbitrary $\varepsilon' > 0$ when $N$ is sufficiently large. This proves the corollary. □

Another way of putting the final conclusion of Corollary 4.2.2 is to state that the ordinary arithmetical function $\log f_{\max}(N)$ itself has the maximum

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

order of magnitude

$$\frac{N}{\log N}(\log \tau)(\log q).$$

By essentially the same arguments as those used in [AB], Chapter 5, §2, it may be verified that Corollary 4.2.2 leads to the following conclusions about the particular functions $d$, $d_*$, $\beta$ and $\omega$:

(4.2.3) THEOREM.

*(i)* $\limsup\limits_{N\to\infty} \dfrac{\log N}{N \log q} \log d_{\max}(N) = \log 2;$

*(ii)* $\limsup\limits_{N\to\infty} \dfrac{\log N}{N \log q} \log d_{*\max}(N) = \log 2;$

*(iii)* $\limsup\limits_{N\to\infty} \dfrac{\log N}{N \log q} \log \beta_{\max}(N) = \dfrac{1}{3} \log 3;$

*(iv)* $\limsup\limits_{N\to\infty} \dfrac{\log N}{N \log q} \omega_{\max}(N) = 1.$ □

Now consider the generalized divisor function $d_k$, and also the generalized unitary-divisor function $d_{*k}$ such that $d_{*k}(a)$ is the total number of ordered $k$-tuples $(b_1, \ldots, b_k)$ of pair-wise *coprime* elements $b_i \in \mathcal{G}$ with product $b_1 b_2 \ldots b_k = a \in \mathcal{G}$.

(4.2.4) THEOREM. *For $k \geq 2$,*

$$\begin{aligned} \limsup_{N\to\infty} \frac{\log N}{N \log q} \log d_{k_{\max}}(N) &= \limsup_{N\to\infty} \frac{\log N}{N \log q} \log d_{*k_{\max}}(N) \\ &= \log k. \end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

PROOF. It was noted in [AB], Chapter 2, §6 that $d_k$ is a *PIM*-function, and that, within the "Dirichlet algebra" $\mathrm{Dir}(\mathcal{G})$, $d_k(z) = [\zeta_G(z)]^k$. By Corollary 2.4.2 of [AB], this equation for $d_k(z)$ implies that

$$\sum_{r=0}^{\infty} d_k(p^r)p^{-rz} = \left(1 - p^{-z}\right)^{-k} \quad \{p \in \mathcal{P}\},$$

and hence that

$$d_k(p^r) = \binom{-k}{r}(-1)^r = \binom{r+k-1}{k-1}.$$

(The last equations can also be derived *directly*, by observing that $d_k(p^r)$ is equal to the total number of partitions of $r$ into exactly $k$ positive summands.) Thus

$$d_k(p^r) = O\left(r^{k-1}\right) \leq e^{B\sqrt{r}},$$

for a suitable constant $B > 0$. Also

$$\binom{r+k-1}{k-1} = \binom{k+r-1}{r} = \frac{k+r-1}{r}\,\frac{k+r-2}{r-1}\cdots\frac{k}{1} \leq k^r,$$

since $k+i \leq (i+1)k$ for $i = 0, 1, \ldots, r-1$. This shows that condition *(ii)* of Corollary 4.2.2 is satisfied by $d_k$, with $t = 1$ and $\tau = k = d_k(p)$. Therefore the stated conclusion about $d_{k_{\max}}(N)$ follows from Corollary 4.2.2.

Next consider:

(4.2.5) LEMMA. *For any $a \in \mathcal{G}$,*

$$d_{*k}(a) = d_k(a_*) = k^{\omega(a)},$$

*where $a_*$ is the "core" ("greatest" square-free divisor) of $a$.*

PROOF. (This lemma *does not* depend on Axiom $\mathcal{A}^{\#}$.) Firstly, the assertions are obvious for $a = 1 \in \mathcal{G}$. Next, for $a = p_1^{r_1}p_2^{r_2}\ldots p_m^{r_m}$ where

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

the $p_i \in \mathcal{P}$ are distinct and $r_i \geq 1$, we have $a_* = p_1 p_2 \dots p_m$. Then, if $b_1 b_2 \dots b_k = a_*$, the elements $b_i \in \mathcal{G}$ must be mutually coprime. Hence

$$d_{*k}(a_*) = d_k(a_*) = k^m = k^{\omega(a)},$$

since $d_k$ is multiplicative, and $d_k(p_i) = k$.

Next suppose that $b_1 b_2 \dots b_k = a$, where the $b_i$ are mutually coprime. In that case, any $b_i \neq 1$ must be a product of one or more powers $p_j^{r_j}$. Thus there is a 1–1 correspondence $b_i \leftrightarrow c_i = b_{i*}$ between those $k$–tuples $(b_1, \dots, b_k)$ of pair–wise coprime elements $b_i$ with $b_1 b_2 \dots b_k = a$ and all $k$–tuples $(c_1, \dots, c_k)$ such that $c_1 c_2 \dots c_k = a_*$. Therefore

$$d_{*k}(a) = d_k(a_*) = k^{\omega(a)}. \qquad \square$$

By Lemma 4.2.5, it is now clear that $d_{*k}$ is a *PIM*–function, with $d_{*k}(p^r) = k$ for any prime–power $p^r \neq 1$ in $\mathcal{G}$. Hence $d_{*k}$ satisfies all the conditions of Corollary 4.2.2, and Theorem 4.2.4 follows. $\square$

Although Corollary 4.2.2 suffices for the present applications to explicit examples of arithmetical functions, it is at least of theoretical interest to record some extensions of Theorem 4.2.1 and Corollary 4.2.2 for more general *PIM*–functions:

(4.2.6) THEOREM. *Let $\mathcal{H}$ denote an arithmetical semigroup such that*

$$N_H(x) = O(x^\delta) \text{ as } x \to \infty, \text{ and } \theta_H(x) > Cx^\delta,$$

*where $\delta$, $C$ are positive constants, and*

$$\theta_H(x) = \sum_{\text{prime } p,\, |p| \leq x} \log |p|.$$

*Let $f$ denote a non-negative real-valued PIM-function on $\mathcal{H}$ such that (for some constant $B > 0$) $f(p^r) \leq e^{B\sqrt{r}}$ for every prime-power $p^r$ in $\mathcal{H}$, and let*

$$\tau = \sup\left\{[f(p^r)]^{\delta/r} : p \textit{ prime in } \mathcal{H},\ r \geq 1\right\}.$$

*Then* $\log f(a)$ *has the maximum order of magnitude*

$$\frac{(\log \tau)(\log |a|)}{\log\log |a|}.$$

Proof. This theorem is essentially a special case of Corollary 5.2.8 of [AB], whose proof was based on two auxiliary results. The first of these ([AB], page 135) implies that

$$\limsup_{|a|\to\infty} \frac{\log f(a)}{\log |a| / \log\log |a|} \leq \delta \log \rho,$$

for any $\rho \geq 1$ such that $\rho^\delta \geq \tau$. However, if $\tau < 1$ then $f(a) < 1$ for $a \neq 1$, and so the inequality

$$\limsup_{|a|\to\infty} \frac{\log f(a)}{\log |a| / \log\log |a|} \leq \log \tau$$

is clear in that case.

On the other hand, for a prime-independent function $f$ with the given properties, the second auxiliary result referred to ([AB], page 136) implies that, for every positive integer $t$ and any prime $p$ in $\mathcal{H}$,

$$\frac{\delta}{t} \log f(p^t) \leq \limsup_{|a|\to\infty} \frac{\log f(a)}{\log |a| / \log\log |a|}.$$

Therefore

$$\limsup_{|a|\to\infty} \frac{\log f(a)}{\log |a| / \log\log |a|} = \log \tau. \qquad \square$$

By an argument similar to that used for Corollary 4.2.2 earlier, one may now deduce:

(4.2.7) COROLLARY. *Let $f$ denote a non-negative real-valued PIM-function on $\mathcal{G}$ such that, for some constant $B > 0$, $f(p^r) < e^{B\sqrt{r}}$ for every prime-power $p^r$ in $\mathcal{G}$, and let*

$$\tau = \sup\left\{[f(p^r)]^{1/r} : p \in \mathcal{P},\ r \geq 1\right\}.$$

*Then $\log f(a)$ has the maximum order of magnitude*

$$\frac{(\log \tau)(\log |a|)}{\log \log |a|},$$

*and*

$$\limsup_{N\to\infty} \frac{\log N}{N \log q} \log f_{\max}(N) = \log \tau. \qquad \square$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

# CHAPTER 5

# ABSTRACT PRIME NUMBER THEOREMS (II)

## 5.1 A Theorem of Indlekofer–Manstavicius–Warlimont

The abstract prime number theorems of Chapter 3 are theorems in the "classical" sense, in that the main asymptotic estimates are of the form $P(m) \sim \frac{q^m}{m}$, or, equivalently, $\bar{\Lambda}(m) \sim q^m$. Further investigation also reveals the existence under suitable conditions of alternative asymptotic estimates of the form either $\bar{\Lambda}(m) \sim q^m$, or $\bar{\Lambda}(m) \sim (1 + (-1)^{m+1})\, q^m$; equivalently either $P(m) \sim \frac{q^m}{m}$ or $P(m) \sim (1 + (-1)^{m+1})\, \frac{q^m}{m}$. Indlekofer, Manstavicius and Warlimont [1] first investigated an abstract prime number theorem of this non–classical type. Such new theorems are novel and deserve further investigation because they also have interesting consequences (see Chapter 6 below).

Consider again Axiom $\mathcal{A}^{\#}$, that there exist constants $A > 0$, $q > 1$, and $\nu$ with $0 \leq \nu < 1$ such that

$$G(n) = Aq^n + O(q^{\nu n}). \tag{1.1}$$

Then Proposition 1.2.1 implies that the generating function $Z(y)$ has an analytic continuation in the disk $\{|y| < q^{-\nu}\}$, as a meromorphic function with the only singularity being a pole of order one at $y = q^{-1}$. From

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Lemma 3.5.2, either $Z(y)$ has no zeros on the circle $|y| = q^{-1}$, or it has a single zero (of order one) on this circle, at $y = -q^{-1}$. In the first case, by Theorem 3.4.5, we have an abstract prime number theorem in the classical sense, with

$$\bar{\Lambda}(n) = q^n + O(q^{\theta n})$$

for some $\theta$ with $\nu \leq \theta < 1$. In the second case, $Z_1(y) = \frac{1-qy}{1+qy} Z(y)$ is holomorphic in the disk $\{|y| \leq q^{-\nu}\}$, and has no zeros in the disk $\{|y| \leq q^{-1}\}$. Therefore there exists some constant $\theta_1$ with $\nu \leq \theta_1 < 1$ such that $Z_1(y)$ has no zeros in $\left\{|y| < q^{-\theta_1}\right\}$. If we shift the integration path in the formula

$$\begin{aligned} \bar{\Lambda}(n) &= \frac{1}{2\pi i} \int_{|y|=r} \frac{Z'(y)}{Z(y)} y^{-n} dy \\ &= q^n \left(1 + (-1)^{n+1}\right) + \frac{1}{2\pi i} \int_{|y|=r} \frac{Z_1'(y)}{Z_1(y)} y^{-n} dy \qquad (1.2) \end{aligned}$$

with $0 < r < q^{-1}$ to a circle $|y| = q^{-\theta}$ with $\theta_1 < \theta < 1$, then we obtain

$$\bar{\Lambda}(n) = q^n \left(1 + (-1)^{n+1}\right) + O\left(q^{\theta n}\right).$$

This is also an abstract prime number theorem of non-classical type. The following theorem of Indlekofer–Manstavicius–Warlimont [1] gives a deeper analysis in this case.

(5.1.1) THEOREM. *Assume Axiom $\mathcal{A}^{\#}$ as before. If $Z(y)$ has a zero at $y = -q^{-1}$, then it has no other zeros in the disk $\{|y| < q^{-\nu}\}$. In this case*

$$\bar{\Lambda}(n) = q^n \left(1 + (-1)^{n+1}\right) + O_\theta\left(q^{\theta n}\right) \qquad (1.3)$$

*for every $\theta$ with $\nu < \theta < 1$.*

The proof of Theorem 5.1.1 will be based on the following lemma which is a special form of *Dirichlet's approximation theorem*:

(5.1.2) LEMMA. *Let $\alpha_1, \dots, \alpha_n$ be real numbers. Given any positive integers $T$ and $M$, there exist an integer $h$ satisfying $T \le h \le TM^n$, and integers $k_1, \dots, k_n$ such that*

$$|\alpha_i h - k_i| \le \frac{1}{M}, \quad i = 1, \dots, n. \tag{1.4}$$

PROOF. Let $I$ denote the unit interval $[0,1]$, and let $I^n$ be the unit cube in $n$–dimension Euclidean space $\mathbb{R}^n$. Divide $I^n$ into $M^n$ cubes of side length $\frac{1}{M}$. Let $\alpha = (\alpha_1, \dots, \alpha_n)$, regarded as a point in $\mathbb{R}^n$, and consider the sequence of points

$$(mT\alpha_1 - [mT\alpha_1], \dots, mT\alpha_n - [mT\alpha_n]), \quad m = 1, 2, \dots, M^n + 1,$$

which are all in the unit cube $I^n$, where $[a]$ denotes the largest integer not exceeding $a$. There are $M^n + 1$ points and $M^n$ small cubes. Thus at least one small cube contains two points. Say that $m' < m$ and points $(m'T\alpha_1 - [m'T\alpha_1], \dots, m'T\alpha_n - [m'T\alpha_n])$ and $(mT\alpha_1 - [mT\alpha_1], \dots, mT\alpha_n - [mT\alpha_n])$ lie in the same small cube. Let $h = T(m - m')$ and $k_i = [mT\alpha_i] - [m'T\alpha_i]$, $i = 1, \dots, n$. Then $h$ is an integer satisfying $T \le h \le TM^n$ and

$$\begin{aligned} |h\alpha_i - k_i| &= |(mT\alpha_i - [mT\alpha_i]) - (m'T\alpha_i - [m'T\alpha_i])| \\ &\le \frac{1}{M}. \quad \square \end{aligned}$$

We next prove the following lemma by using Dirichlet's approximation theorem:

(5.1.3) LEMMA. *Let $\alpha_1, \dots, \alpha_n$ be real numbers and $\beta_1, \dots, \beta_n$ be positive real numbers. Then*

$$\limsup_{m \to \infty} \sum_{i=1}^{n} \beta_i \cos(2m\pi\alpha_i) = \sum_{i=1}^{n} \beta_i.$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

PROOF. Plainly,

$$\limsup_{m\to\infty}\sum_{i=1}^{n}\beta_i\cos(2m\pi\alpha_i)\le\sum_{i=1}^{n}\beta_i,$$

since $\beta_1,\ldots,\beta_n$ are positive. It suffices to show that there exists a sequence of positive integers $m_h,\ h=1,2,\ldots$, such that

$$\lim_{h\to\infty}\sum_{i=1}^{n}\beta_i\cos(2m_h\pi\alpha_i)=\sum_{i=1}^{n}\beta_i. \tag{1.5}$$

Actually, by Lemma 5.1.2, there exist an integer $m_h$ satisfying $h\le m_h\le h^{n+1}$ and integers $k_{1,h},\ldots,k_{n,h}$ such that

$$|\alpha_i m_h-k_{i,h}|\le\frac{1}{h},\quad i=1,\ldots,n. \tag{1.6}$$

Hence

$$\sum_{i=1}^{n}\beta_i\cos(2m_h\pi\alpha_i)=\sum_{i=1}^{n}\beta_i\cos\left(2\pi(\alpha_i m_h-k_{i,h})\right),$$

and so (1.5) follows from (1.6) as $h\to\infty$. □

PROOF OF THEOREM 5.1.1. We shall show that if $Z(y)$ has a zero at $y=-q^{-1}$ then it has no other zeros in the disk $\{|y|<q^{-\nu}\}$. Then (1.3) follows from the formula (1.2), by shifting the integration path to a circle $|y|=q^{-\theta}$ with $\nu<\theta<1$.

Suppose on the contrary to our assertion that $Z(y)$ has some zeros in the annulus $\{q^{-1}<|y|<q^{-\nu}\}$. Let $\rho$ be the minimum of the moduli of these zeros, and let $\rho e^{2\pi i\alpha_j},\ j=1,\ldots,n$ denote all those zeros with modulus $\rho$. Then there exists a number $\eta$ with $\rho<\eta<q^{-\nu}$, such that there exist no zeros of $Z(y)$ in the annulus $\{\rho<|y|\le\eta\}$. If we shift the integration path in the formula

$$\bar{\Lambda}(m)=\frac{1}{2\pi i}\int_{|y|=r}\frac{Z'(y)}{Z(y)}y^{-m}dy$$

with $0 < r < q^{-1}$ to the circle $|y| = \eta$, then we have

$$\begin{aligned}\bar{\Lambda}(m) &= q^m\left(1+(-1)^{m+1}\right) - \sum_{j=1}^{n}(\rho e^{2\pi i\alpha_j})^{-m} \\ &\quad + \frac{1}{2\pi i}\int_{|y|=\eta}\frac{Z'(y)}{Z(y)}y^{-m}dy \\ &= q^m\left(1+(-1)^{m+1}\right) - \rho^{-m}\sum_{j=1}^{n}e^{-2m\pi i\alpha_j} + O(\eta^{-m}),\end{aligned}$$

and therefore

$$\bar{\Lambda}(2m) = -\rho^{-2m}\sum_{j=1}^{n}e^{-4m\pi i\alpha_j} + O(\eta^{-2m}).$$

Note that the $\rho e^{-2\pi i\alpha_j}$ are also zeros of $Z(y)$. Hence

$$\begin{aligned}&\rho^{-2m}\sum_{j=1}^{n}e^{-4m\pi i\alpha_j} \\ &\quad = \frac{1}{2}\left[\rho^{-2m}\sum_{j=1}^{n}e^{-4m\pi i\alpha_j} + \rho^{-2m}\sum_{j=1}^{n}e^{4m\pi i\alpha_j}\right] \\ &\quad = \rho^{-2m}\sum_{j=1}^{n}\cos(4m\pi\alpha_j).\end{aligned}$$

It follows that

$$\bar{\Lambda}(2m) = -\rho^{-2m}\sum_{j=1}^{n}\cos(4m\pi\alpha_j) + O(\eta^{-2m}). \qquad (1.7)$$

Note that $0 < \rho < \eta$. Combining it with Lemma 5.1.3, (1.7) implies that there exist infinitely many $m$ sufficiently large such that

$$\bar{\Lambda}(2m) \le -\frac{n}{2}\rho^{-2m} < 0.$$

This is certainly absurd, since $\bar{\Lambda}(m)$ is non–negative. □

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

## 5.2 The Total Number of Zeros of the Generating Function

Abstract prime number theorems of the above alternative forms give rise to a fundamental question: what conditions ensure such alternative asymptotic estimates? If Axiom $\mathcal{A}^{\#}$ is assumed, then, from Lemma 3.5.2, $Z(y)$ has either no zeros, or only a zero $y = -q^{-1}$ of order one on the circle $|y| = q^{-1}$, *and in that case* an alternative asymptotic estimate follows. Hence the real question here is: what weaker or other conditions will ensure an alternative asymptotic estimate?

To start to answer this question, we begin with an investigation of the zeros of $Z(y)$ on the circle $|y| = q^{-1}$. Assume that there exist constants $A > 0$, $q > 1$, and $\gamma > 1$ such that

$$G(n) = Aq^n + O\left(q^n n^{-\gamma}\right), \quad n = 1, 2, \ldots . \tag{2.1}$$

Then the generating function $Z(y)$ is continuous in the closed disk $\{|y| \leq q^{-1}\}$. It has no zeros in the open disk $\{|y| < q^{-1}\}$, but may have zeros on the circle $|y| = q^{-1}$.

If $q^{-1}e^{2\pi i\theta}$ is a zero of $Z(y)$, where $\theta$ is a real number, the real number

$$\alpha(\theta) := \sup\left\{\alpha : \limsup_{r \to q^{-1}-} \left(q^{-1} - r\right)^{-\alpha} \left|Z\left(re^{2\pi i\theta}\right)\right| < \infty\right\} \tag{2.2}$$

is called, by definition, the **order** of $q^{-1}e^{2\pi i\theta}$. Note that $\alpha(\theta)$ is non-negative, but need not be a positive integer. An equivalent definition is

$$\alpha(\theta) := \liminf_{r \to q^{-1}-} \frac{\log|Z(re^{2\pi i\theta})|}{\log\left(q^{-1} - r\right)} \tag{2.3}$$

which may be seen as follows: On the one hand, if

$$\limsup_{r \to q^{-1}-} \left(q^{-1} - r\right)^{-\alpha} \left|Z\left(re^{2\pi i\theta}\right)\right| < \infty$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

then

$$\left(q^{-1}-r\right)^{-\alpha}\left|Z\left(re^{2\pi i\theta}\right)\right| \leq K_\alpha,$$

and hence

$$\log\left|Z\left(re^{2\pi i\theta}\right)\right| - \alpha\log\left(q^{-1}-r\right) \leq \log K_\alpha.$$

It follows that

$$\frac{\log\left|Z\left(re^{2\pi i\theta}\right)\right|}{\log\left(q^{-1}-r\right)} \geq \alpha + \frac{\log K_\alpha}{\log\left(q^{-1}-r\right)},$$

since $\log\left(q^{-1}-r\right) < 0$ for $r$ sufficiently close to $q^{-1}$. Thus

$$\liminf_{r\to q^{-1}-}\frac{\log\left|Z\left(re^{2\pi i\theta}\right)\right|}{\log\left(q^{-1}-r\right)} \geq \alpha.$$

On the other hand, if

$$\liminf_{r\to q^{-1}-}\frac{\log\left|Z\left(re^{2\pi i\theta}\right)\right|}{\log\left(q^{-1}-r\right)} > \alpha$$

then, for $r$ sufficiently close to $q^{-1}$,

$$\frac{\log\left|Z\left(re^{2\pi i\theta}\right)\right|}{\log\left(q^{-1}-r\right)} > \alpha,$$

and hence

$$\left(q^{-1}-r\right)^{-\alpha}\left|Z\left(re^{2\pi i\theta}\right)\right| < 1.$$

Thus

$$\limsup_{r\to q^{-1}-}\left(q^{-1}-r\right)^{-\alpha}\left|Z\left(re^{2\pi i\theta}\right)\right| < \infty.$$

This shows that

$$\liminf_{r\to q^{-1}-}\frac{\log\left|Z\left(re^{2\pi i\theta}\right)\right|}{\log\left(q^{-1}-r\right)}$$
$$= \sup\left\{\alpha : \limsup_{r\to q^{-1}-}\left(q^{-1}-r\right)^{-\alpha}\left|Z\left(re^{2\pi i\theta}\right)\right| < \infty\right\}.$$

In this section, we shall prove the following theorem which gives the "total number" of zeros of $Z(y)$ on the circle $|y| = q^{-1}$, subject to (2.1) above (cf. Zhang [6]).

(5.2.1) THEOREM. *Suppose that (2.1) holds. Then the "total number" of zeros of $Z(y)$ on the circle $|y| = q^{-1}$ is at most one, in the sense that*

$$\alpha\left(\frac{1}{2}\right) + 2\sum_{0<\theta<\frac{1}{2}} \alpha(\theta) \leq 1 \tag{2.4}$$

*or*

$$2\sum_{0<\theta<\frac{1}{2}} \alpha(\theta) \leq 1, \tag{2.5}$$

*according as $-q^{-1}$ is or is not a zero of $Z(y)$, where the summation is taken over all zeros of $Z(y)$ on the upper half of the circle $|y| = q^{-1}$.*

*Remark.* We note that $\alpha\left(\frac{1}{2}\right)$ is the order of the zero $-q^{-1}$. The upper bound of the total number of zeros given in (2.4) and (2.5) is the best possible as Examples 3.8.1 of Chapter 3 shows.

We shall first prove the following more general formulation of Theorem 5.2.1, and then deduce Theorem 5.2.1.

(5.2.2) THEOREM. *Let $f(z)$ be a function continuous on $\{z \in \mathbb{C} : |z| \leq 1 \text{ and } z \neq 1\}$, and holomorphic in the disk $\{|z| < 1\}$. Suppose that $f(z)$ has no zeros in this disk. Also suppose that*

$$\log f(z) = \sum_{k=1}^{\infty} c_k z^k, \quad |z| < 1, \tag{2.6}$$

*with coefficients $c_k \geq 0$, and that, for some constant $\tau > 0$,*

$$\lim_{r\to 1-} f(r)(1-r)^{\tau} \tag{2.7}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

*exists and is positive. Let* $0 < \theta_1 < \cdots < \theta_k < 1$ *be arbitrary. Then*

$$\sum_{j=1}^{k} \liminf_{r \to 1-} \frac{\log \left| f\left(re^{2\pi i \theta_j}\right)\right|}{\log(1-r)} \leq \tau. \tag{2.8}$$

To prove Theorem 5.2.2, we begin with the representation of the solution set of the diophantine equation $\alpha_1\theta_1 + \cdots + \alpha_k\theta_k = m$.

(5.2.3) LEMMA. *Given* $\theta = (\theta_1, \ldots, \theta_k) \in \mathbb{R}^k$ *with* $0 < \theta_1 < \cdots < \theta_k < 1$ *arbitrary, let*

$$S = S(\theta) := \left\{\alpha = (\alpha_1, \ldots, \alpha_k) \in \mathbb{Z}^k : \langle \alpha, \theta \rangle \in \mathbb{Z}\right\}, \tag{2.9}$$

*where* $\langle \alpha, \theta \rangle = \alpha_1\theta_1 + \cdots + \alpha_k\theta_k$. *If* $S \neq \{0\}$ *then there exist a positive integer* $m \leq k$ *(m is the "dimension" of S), and a matrix* $C = C(\theta) \in \mathbb{M}\,(m \times k, \mathbb{Q})$ *of rank m such that*

$$S = \{\beta C : \beta \in \mathbb{Z}^m\}.$$

PROOF. We consider two possible cases separately.

*Case I: The equation* $\alpha_1\theta_1 + \cdots + \alpha_k\theta_k = z$ *has no solutions in* $\mathbb{Z}^k$ *for all* $z \in \mathbb{Z}$, $z \neq 0$. Then the homogeneous equation $\alpha_1\theta_1 + \cdots + \alpha_k\theta_k = 0$ has non-zero solutions, since $S \neq \{0\}$. We consider a maximal subset of elements, linearly independent over $\mathbb{Q}$, of the set $\{\theta_1, \ldots, \theta_k\}$. Upon changing the subscripts, we may assume that $\{\theta_1, \ldots, \theta_\ell\}$ is such a subset. Then $\ell < k$. There exist $a_{s,t} \in \mathbb{Q}$, $t = 1, \ldots, \ell$, $s = \ell + 1, \ldots, k$ such that

$$\begin{aligned} \theta_{\ell+1} &= a_{\ell+1,1}\theta_1 + \cdots + a_{\ell+1,\ell}\theta_\ell, \\ &\vdots \\ \theta_k &= a_{k,1}\theta_1 + \cdots + a_{k,\ell}\theta_\ell. \end{aligned} \tag{2.10}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

If $\alpha \in S$, then

$$\begin{aligned} 0 &= \alpha_1\theta_1 + \cdots + \alpha_k\theta_k \\ &= (\alpha_1 + \alpha_{\ell+1}a_{\ell+1,1} + \cdots + \alpha_k a_{k,1})\,\theta_1 + \cdots \\ &\qquad + (\alpha_\ell + \alpha_{\ell+1}a_{\ell+1},+ \cdots + \alpha_k a_{k,\ell})\,\theta_\ell. \end{aligned}$$

It follows that

$$\begin{aligned} \alpha_1 + \alpha_{\ell+1}a_{\ell+1,1} + \cdots + \alpha_k a_{k,1} &= 0, \\ &\vdots \\ \alpha_\ell + \alpha_{\ell+1}a_{\ell+1,\ell} + \cdots + \alpha_k a_{k,\ell} &= 0 \end{aligned}$$

and hence

$$\begin{aligned} \alpha_1 &= -\alpha_{\ell+1}a_{\ell+1,1} - \cdots - \alpha_k a_{k,l}, \\ &\vdots \\ \alpha_\ell &= -\alpha_{\ell+1}a_{\ell+1,1} - \cdots - \alpha_k a_{k,\ell}. \end{aligned}$$

Let $m = k - \ell$ and

$$C = \begin{bmatrix} -a_{\ell+1,1} & \cdots & -a_{\ell+1,\ell} & 1 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ -a_{k,1} & \cdots & -a_{k,\ell} & 0 & \cdots & 1 \end{bmatrix}.$$

Then $S = \{\beta C : \beta \in \mathbb{Z}^m\}$. Obviously, the rank of $C$ is $m$.

*Case II: The equation $\alpha_1\theta_1 + \cdots + \alpha_k\theta_k = z$ has solution in $\mathbb{Z}^k$ for some $z \in \mathbb{Z}$, $z \neq 0$.* Then the set $M = \{z :\ 0 < z = \langle\alpha, \theta\rangle$ for some $\alpha \in S\}$ is non–empty. Let $z_0 = \min\{z : z \in M\}$ and $\alpha^0 = (\alpha_1^0, \ldots, \alpha_k^0) \in S$, such that $\alpha_1^0\theta_1 + \cdots + \alpha_k^0\theta_k = z_0$. We claim that, for each $\alpha \in \mathbb{Z}^k$, $\alpha \in S$ if and only if there exist $t \in \mathbb{Z}$ and $\eta = (\eta_1, \ldots, \eta_k) \in \mathbb{Z}^k$ such that $\alpha = t\alpha^0 + \eta$ and

$$\eta_1\theta_1 + \cdots + \eta_k\theta_k = 0,$$

and claim that if $\alpha \in S$ then the representation $\alpha = t\alpha^0 + \eta$ is unique. Actually, if $\alpha_1\theta_1 + \cdots + \alpha_k\theta_k = 0$, then $\alpha = 0 \cdot \alpha^0 + \eta$ with $\eta = \alpha$. If $\alpha_1\theta_1 + \cdots + \alpha_k\theta_k = z \in \mathbb{Z}$ and $z \neq 0$, then $z = tz_0$ for some $t \in \mathbb{Z}$. Otherwise, $z = tz_0 + r$ with $t$, $r \in \mathbb{Z}$ and $0 < r < z_0$. Then $\alpha' = \alpha - t\alpha^0 \in \mathbb{Z}^k$ and

$$\langle \alpha', \theta \rangle = z - tz_0 = r.$$

This contradicts the definition of $z_0$. Thus $z = tz_0$, and $\eta = \alpha - t\alpha^0$ satisfies $\langle \eta, \theta \rangle = 0$. Clearly, $t$ and $\eta$ are unique and the claims hold.

Now, if the homogeneous equation $\alpha_1\theta_1 + \cdots + \alpha_k\theta_k = 0$ has only the solution $(0, \ldots, 0) \in \mathbb{Z}^k$, then $\eta = 0$ and $\alpha = t\alpha^0$. Let $m = 1$, $C = \alpha^0$ and then $S = \{\beta C : \beta \in \mathbb{Z}\}$.

Thus we may assume that the homogeneous equation $\alpha_1\theta_1 + \cdots + \alpha_k\theta_k = 0$ has non–zero solutions in $\mathbb{Z}^k$. Then, as in Case I, we may assume that $\{\theta_1, \ldots, \theta_\ell\}$ is a maximal subset of elements, linearly independent over $\mathbb{Q}$, of the set $\{\theta_1, \ldots, \theta_k\}$, and that there exist $a_{s,t}$, $t = 1, \ldots, \ell$, $s = \ell + 1, \ldots, k$ such that (2.10) holds. Let $m = k - \ell + 1$ and

$$C = \begin{bmatrix} \alpha_1^0 & \cdots & \alpha_{k-\ell}^0 & \alpha_{k-\ell+1}^0 & \cdots & \alpha_k^0 \\ -a_{\ell+1,1} & \cdots & -a_{\ell+1,\ell} & 1 & \cdots & 0 \\ \vdots & & \vdots & \vdots & \ddots & \vdots \\ -a_{k,1} & \cdots & -a_{k,\ell} & 0 & \cdots & 1 \end{bmatrix}.$$

Then $S = \{\beta C : \beta \in \mathbb{Z}^m\}$. Finally, the rank of $C$ is $m = k - \ell + 1$, since the first row of $C$ is linearly independent of other rows. □

We now turn to the proof of Theorem 5.2.2:

For $x = (x_1, \ldots, x_k) \in \mathbb{R}^k$, $y = (y_1, \ldots, y_k) \in \mathbb{R}^k$, we set $\|x\| = \max_{1 \leq j \leq k} |x_j|$ and $\langle x, y \rangle = x_1y_1 + \cdots + x_ky_k$. Let $K$ be a positive integer. We consider the inequaltiy

$$0 \le \left| \sum_{\substack{\ell\in\mathbb{N}^k \\ \|\ell\|\le K}} e^{i\langle \ell, x\rangle} \right|^2 = \sum_{\alpha\in\mathbb{Z}^k} n(\alpha, K)\cos\langle \alpha, x\rangle, \tag{2.11}$$

where $\alpha = (\alpha_1, \dots, \alpha_k)$ and

$$n(\alpha, K) := \sum_{\substack{\ell,\ell'\in\mathbb{N}^k \\ \|\ell\|,\,\|\ell'\|\le K \\ \ell-\ell'=\alpha}} 1 = \begin{cases} 0, & \text{if } \|\alpha\| \ge K, \\ \prod_{j=1}^{k} (K - |\alpha_j|), & \text{if } \|\alpha\| < K. \end{cases} \tag{2.12}$$

*Proof of Theorem 5.2.2* Let $x = 2\pi m(\theta_1, \dots, \theta_k)$ with $m \in \mathbb{N}$, in (2.11). We multiply both sides of (2.11) by $c_m r^m$ and sum over $m$. Then from (2.6), for $0 < r < 1$,

$$\begin{aligned} 0 \ &\le \ \sum_{\alpha\in\mathbb{Z}^k} n(\alpha, K)\log\left|f(re^{2\pi i\langle\alpha,\theta\rangle})\right| \\ &= \left( \sum_{\substack{\alpha\in\mathbb{Z}^k \\ \langle\alpha,\theta\rangle\in\mathbb{Z}}} n(\alpha, K) \right) \log f(r) \\ &\qquad + \sum_{\substack{\alpha\in\mathbb{Z}^k \\ \langle\alpha,\theta\rangle\notin\mathbb{Z}}} n(\alpha, K)\log\left|f(re^{2\pi i\langle\alpha,\theta\rangle})\right|. \end{aligned} \tag{2.13}$$

It follows that

$$\sum_{\substack{\alpha\in\mathbb{Z}^k \\ \langle\alpha,\theta\rangle\notin\mathbb{Z}}} n(\alpha, K)\frac{\log\left|f(re^{2\pi i\langle\alpha,\theta\rangle})\right|}{\log(1-r)} \le \left( \sum_{\substack{\alpha\in\mathbb{Z}^k \\ \langle\alpha,\theta\rangle\in\mathbb{Z}}} n(\alpha, K) \right) \frac{\log f(r)}{\log\frac{1}{1-r}}. \tag{2.14}$$

Let

$$N(\theta, K) := \sum_{\substack{\alpha\in\mathbb{Z}^k \\ \langle\alpha,\theta\rangle\in\mathbb{Z}}} n(\alpha, K) = \sum_{\alpha\in S} n(\alpha, K),$$

where $S$ is defined in (2.9), and

$$N_j(\theta, K) := \sum_{\substack{\alpha\in\mathbb{Z}^k \\ \langle\alpha,\theta\rangle-\theta_j\in\mathbb{Z}}} n(\alpha, K) = \sum_{\alpha\in S_j} n(\alpha, K), \quad j = 1, \ldots, k, \tag{2.15}$$

where

$$S_j = S_j(\theta) := \{\alpha \in \mathbb{Z}^k : \langle\alpha, \theta\rangle - \theta_j \in \mathbb{Z}\}, \quad j = 1, \ldots, k.$$

Note that $S, S_j, j = 1, \ldots, k$ are mutually disjoint, and that

$$S_j = \{\alpha + e_j : \alpha \in S\}, \quad j = 1, \ldots, k,$$

where $e_j$ is the $j$th vector of the standard basis of $\mathbb{R}^k$. From (2.14), we have

$$\begin{aligned} &\sum_{j=1}^{k} \frac{N_j(\theta, K)}{N(\theta, K)} \frac{\log\left|f(re^{2\pi i\theta_j})\right|}{\log(1-r)} \\ &\qquad + \sum_{\substack{\alpha\in\mathbb{Z}^k \\ \alpha\notin S\cup\left(\bigcup_{j=1}^{k} S_j\right)}} \frac{n(\alpha, K)}{N(\theta, K)} \frac{\log\left|f(re^{2\pi i\langle\alpha,\theta\rangle})\right|}{\log(1-r)} \\ &\le \frac{\log f(r)}{\log\frac{1}{1-r}}. \end{aligned} \tag{2.16}$$

Note that, from (2.7),

$$\lim_{r\to1-} \frac{\log f(r)}{\log\frac{1}{1-r}} = \tau,$$

and that

$$\liminf_{r\to1-} \frac{\log\left|f(re^{2\pi i\langle\alpha,\theta\rangle})\right|}{\log(1-r)} \ge 0$$

for $\langle\alpha, \theta\rangle \notin \mathbb{Z}$, since $f(z)$ is continuous on $\{z \in \mathbb{C} : |z| \le 1, z \ne 1\}$. It follows, from (2.16), that

$$\sum_{j=1}^{k} \frac{N_j(\theta, K)}{N(\theta, K)} \liminf_{r\to1-} \frac{\log\left|f(re^{2\pi i\theta_j})\right|}{\log(1-r)} \le \tau. \tag{2.17}$$

We claim that

$$\frac{N_j(\theta, K)}{N(\theta, K)} = 1 + O(K^{-1}), \quad j = 1, \ldots, k. \tag{2.18}$$

Actually, if $S = \{0\}$, from (2.12), we have

$$N(\theta, K) = n(0, K) = K^k$$

and

$$N_j(\theta, K) = n(e_j, K) = K^{k-1}(K-1).$$

If $S \neq \{0\}$, by Lemma 5.2.3, there exists a matrix $C = C(\theta) \in \mathbb{M}(m \times k, \mathbb{Q})$ of rank $m > 0$ such that $S = \{\beta C : \beta \in \mathbb{Z}^m\}$. We note that

$$\sum_{\substack{\beta \in \mathbb{Z}^m \\ \|\beta C\| \leq K}} 1 \gg_\theta K^m$$

since $\|\beta C\| \leq \|\beta\| \sum_{i=1}^m \sum_{j=1}^k |c_{ij}|$. Hence

$$N(\theta, K) = \sum_{\substack{\beta \in \mathbb{Z}^m \\ \|\beta C\| \leq K}} \prod_{j=1}^k (K - |\beta C_j|) \gg_\theta K^{m+k},$$

where $C_j$ is the $j$th column of $C$. Also,

$$\begin{aligned} N_j(\theta, K) &= \sum_{\substack{\beta \in \mathbb{Z}^m \\ \|\beta C + e_j\| \leq K}} \left( \prod_{\substack{i=1 \\ i \neq j}}^k (K - |\beta C_i|) \right) (K - |\beta C_j + 1|) \\ &= N(\theta, K) + O(K^{m+k-1}), \end{aligned}$$

$j = 1, \ldots, k$. Thus the claim holds.

Now, (2.8) follows from (2.17) and (2.18), by letting $K \to \infty$ on the left-hand side of (2.17). □

*Proof of Theorem 5.2.1* Consider $f(z) := Z(q^{-1}z)$. Then, from (2.1),

$$f(z) = \frac{Z_0(q^{-1}z)}{1-z},$$

where

$$Z_0(q^{-1}z) = 1 - (1-A)z + (1-z)\sum_{n=1}^{\infty} a_n n^{-\gamma} z^n,$$

with $a_n = O(1)$, is continuous on the disk $\{|z| \leq 1\}$ since $\gamma > 1$, and is holomorphic in the disk $\{|z| < 1\}$, and $Z_0(q^{-1}) = A > 0$. It follows that

$$\lim_{r \to 1-} f(r)(1-r) = A > 0.$$

Also, it is easy to see that

$$\log f(z) = \log Z(q^{-1}z) = \sum_{k=1}^{\infty} \frac{\bar{\Lambda}(k)}{k} q^{-k} z^k, \quad |z| < 1,$$

and so (2.6) holds with $c_k = \bar{\Lambda}(k)k^{-1}q^{-k} \geq 0$.

Thus (2.4) and (2.5) follow from Theorem 5.2.2. □

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

## 5.3 The Orders of the Zeros

If $\gamma > 2$ in (2.1), then the orders of zeros of the generating function $Z(y)$ are positive integers, as the following theorem shows. This theorem (cf. Zhang [6]) is essentially best possible, as Example 5.3.3 will show.

(5.3.1) THEOREM. *Let $q^{-1}e^{2\pi i\theta}$ be a zero of $Z(y)$, with order $\alpha = \alpha(\theta)$ where $0 < \theta < 1$. If (2.1) holds with $\gamma > 1 + \alpha$, in particular, if $\theta \neq \frac{1}{2}$ and (2.1) holds with $\gamma > \frac{3}{2}$, or if $\theta = \frac{1}{2}$ and (2.1) holds with $\gamma > 2$, then $\alpha$ is a positive integer. Moreover,*

$$\lim_{r\to q^{-1}-} \frac{Z\left(re^{2\pi i\theta}\right)}{\left(q^{-1}-r\right)^{\alpha} e^{2\pi i\alpha\theta}} = \frac{(-1)^{\alpha}}{\alpha!} Z^{(\alpha)}\left(q^{-1}e^{2\pi i\theta}\right) \neq 0,$$

*and $Z(y)\left(q^{-1}e^{2\pi i\theta} - y\right)^{\alpha}$ is continuous on the region $\{y : |y| \leq q^{-1}, |y - q^{-1}e^{2\pi i\theta}| < \varepsilon\}$, for some $\varepsilon > 0$.*

As in Section 5.2, we shall first prove a more general theorem, and then deduce the required conclusion:

(5.3.2) THEOREM. *Let $f(z) = S(z) + R(z)$ where $S(z)$ is holomorphic in the disk $\{|z| < 1\}$, and*

$$R(z) = \sum_{n=0}^{\infty} r_n z^n, \quad |z| < 1,$$

*with $r_n = O(n^{-\gamma})$. Suppose that $S(z)$ is continuous on $\{z : |z| \leq 1$ and $z \neq 1\}$, and that for some constant $\tau > 0$,*

$$\lim_{r\to 1-} S(r)(1-r)^{\tau}$$

*exists and is positive. Also suppose that $f(z) \neq 0$ in the disk $\{|z| < 1\}$, and*

$$\log f(z) = \sum_{k=1}^{\infty} c_k z^k, \quad |z| < 1$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

*with coefficients* $c_k \geq 0$. *Let*

$$\alpha = \alpha(\theta) := \sup\left\{\beta :\ (1-r)^{-\beta}|f(re^{2\pi i\theta})| \ll 1\right\}.$$

*If* $\gamma > 1 + \alpha$, *in particular, if* $0 < \theta < 1$, $\theta \neq \frac{1}{2}$, *and* $\gamma > 1 + \frac{\tau}{2}$, *or if* $\theta = \frac{1}{2}$ *and* $\gamma > 1 + \tau$, *then* $\alpha$ *is a positive integer. Moreover,*

$$\lim_{r\to 1-} \frac{f(re^{2\pi i\theta})}{(1-r)^{\alpha} e^{2\pi i\alpha\theta}} = \frac{(-1)^{\alpha}}{\alpha!} f^{(\alpha)}(e^{2\pi i\theta}) \neq 0, \tag{3.1}$$

*and* $f(z)/(e^{2\pi i\theta} - z)^{\alpha}$ *is continuous on* $\{z :\ |z| \leq 1, |z - e^{2\pi i\theta}| < \varepsilon\}$, *for some* $\varepsilon > 0$.

*Proof of Theorem 5.3.2* Without loss of generality, we may assume that $\gamma$ is not an integer. We have to show that $\alpha$ is an integer. Suppose on the contrary that $\alpha$ is not an integer. Then, from the definition of $\alpha$,

$$\lim_{r\to 1-} \frac{|f(re^{2\pi i\theta})|}{(1-r)^{k}} = 0 \tag{3.2}$$

for all integers $k < \alpha$.

Note that all derivatives $f^{(k)}(z)$ with $k < \gamma - 1$ are continuous on $\{z : |z| \leq 1, |z - e^{2\pi i\theta}| < \varepsilon\}$ for some $\varepsilon > 0$. Hence, for $1 \leq k < \gamma - 1$, we have the Taylor formula

$$\begin{aligned} f(re^{2\pi i\theta}) \ &= \ \sum_{n=1}^{k-1} \frac{1}{n!} f^{(n)}(e^{2\pi i\theta}) e^{2\pi i n\theta}(r-1)^{n} \\ &\qquad + \frac{1}{(k-1)!}\int_1^r f^{(k)}(te^{2\pi i\theta}) e^{2\pi i k\theta}(r-t)^{k-1} dt. \end{aligned} \tag{3.3}$$

Moreover, if $k = [\gamma] - 1$, then

$$\begin{aligned} &\left|f^{(k)}(te^{2\pi i\theta}) - f^{(k)}(e^{2\pi i\theta})\right| \\ &\quad = \left|\left(S^{(k)}(te^{2\pi i\theta}) - S^{(k)}(e^{2\pi i\theta})\right) + \left(R^{(k)}(te^{2\pi i\theta}) - R^{(k)}(e^{2\pi i\theta})\right)\right| \\ &\quad \ll (1-t) + (1-t)^{\gamma-[\gamma]} \ll (1-t)^{\gamma-[\gamma]}, \end{aligned}$$

since

$$\begin{aligned}
&\left|R^{(k)}(te^{2\pi i\theta}) - R^{(k)}(e^{2\pi i\theta})\right| \\
&= \left|\sum_{n=k}^{\infty} r_n n(n-1)\dots(n-k+1)e^{2\pi i(n-k)\theta}(1-t^{n-k})\right| \\
&\ll (1-t)\sum_{k\le n<M} n^{-\gamma+k+1} + \sum_{n\ge M} n^{-\gamma+k} \\
&\ll (1-t)M^{-\gamma+k+2} + M^{-\gamma+k+1} \\
&\ll (1-t)^{\gamma-k-1} = (1-t)^{\gamma-[\gamma]}
\end{aligned}$$

with $M = (1-t)^{-1}$. Hence, if $k = [\gamma]-1$, the last term of (3.3) equals

$$\frac{1}{k!} f^{(k)}(e^{2\pi i\theta})e^{2\pi ik\theta}(r-1)^k + O((1-r)^{\gamma-1}),$$

and we obtain

$$\begin{aligned}
f(re^{2\pi i\theta}) &= \sum_{n=1}^{[\gamma]-1} \frac{1}{n!} f^{(n)}(e^{2\pi i\theta})e^{2\pi in\theta}(r-1)^n \\
&\quad +O((1-r)^{\gamma-1}). \qquad (3.4)
\end{aligned}$$

Since $\alpha < \gamma - 1$, from (3.2) and (3.4), we obtain, by induction,

$$f^{(n)}(e^{2\pi i\theta}) = 0 \quad \text{for} \quad 1 \le n \le [\alpha]. \qquad (3.5)$$

Now, from (3.4) and (3.5), if $[\alpha] < [\gamma] - 1$ then

$$\frac{\left|f(re^{2\pi i\theta})\right|}{(1-r)^{[\alpha]+1}} \ll 1,$$

and if $[\alpha] = [\gamma] - 1$ then

$$\frac{\left|f(re^{2\pi i\theta})\right|}{(1-r)^{\gamma-1}} \ll 1.$$

This implies that $\alpha \ge \min\{[\alpha]+1,\ \gamma-1\}$; which contradicts $\alpha < \gamma - 1$. Therefore, $\alpha$ must be a positive integer.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Finally, because $\alpha$ is a positive integer and $\alpha < \gamma - 1$, (3.1) follows from (3.4) since $f^{(n)}(e^{2\pi i\theta}) = 0$ for $1 \leq n < \alpha$, by induction. Moreover, for $z$ in $\{z : |z| \leq 1, |z - e^{2\pi i\theta}| < \varepsilon\}$ with some $\varepsilon > 0$, we have the Taylor formula

$$\begin{aligned} f(z) &= \sum_{n=\alpha}^{k-1} \frac{1}{n!} f^{(n)}(e^{2\pi i\theta})(z - e^{2\pi i\theta})^n \\ &\quad + \frac{1}{(k-1)!} \int_0^1 f^{(k)}\left((1-t)e^{2\pi i\theta} + tz\right)\left(z - e^{2\pi i\theta}\right)^k (1-t)^{k-1} dt \end{aligned}$$

with $k = [\gamma] - 1$, and so the continuity of $f(z)/(e^{2\pi i\theta} - z)^\alpha$ follows. □

*Proof of Theorem 5.3.1* Let $f(z) := Z(q^{-1}z)$. Then we can write $f(z) = S(z) + R(z)$, where

$$S(z) = \frac{A}{1-z} + (1 - A)$$

and

$$R(z) = \sum_{n=1}^{\infty} r_n z^n$$

with $r_n = O(n^{-\gamma})$. Then $S(z)$ is continuous on $\{z : |z| \leq 1 \text{ and } z \neq 1\}$, and

$$\lim_{r \to 1-} S(r)(1 - r) = A > 0.$$

Thus $f(z)$ satisfies the hypotheses of Theorem 5.3.2, and Theorem 5.3.1 follows directly. □

The following example shows that $\alpha\left(\frac{1}{2}\right)$ may not be integral if (2.1) holds with $\gamma < 2$, and hence the result in Theorem 5.3.1 is in some sense essentially "best possible".

(5.3.3) Example. Let $m$ be an arbitrary positive integer such that $m > 4$. Formally set $q = m^2$, $\alpha = \left(\frac{m-1}{m}\right)^2$, and

$$\bar{\Lambda}(n) = q^n \left(1 + (-1)^{n+1}\alpha\right), \quad n = 1, 2, \ldots .$$

Then the $\bar{\Lambda}(n)$ are all positive integers. We have $P(1) = \bar{\Lambda}(1) > 0$ and, for $n \geq 2$,

$$\begin{aligned} P(n) &= \sum_{r|n} \bar{\Lambda}(r)\mu\left(\frac{n}{r}\right) \geq \bar{\Lambda}(n) - \sum_{1 \leq r \leq \frac{n}{2}} \bar{\Lambda}(r) \\ &\geq q^n(1-\alpha) - 2\sum_{1 \leq r \leq \frac{n}{2}} q^r \geq q^{\frac{n}{2}}\left\{q(1-\alpha) - \frac{2q}{q-1}\right\} \\ &\geq q^{\frac{n}{2}}(2m-1-4) > 0. \end{aligned}$$

Thus the $P(n)$ are all positive integer too.

It is easy to see that here

$$y\frac{Z'(y)}{Z(y)} = \Lambda^{\#}(y) = \frac{qy}{1-qy} + \frac{\alpha y}{1+qy},$$

and hence

$$Z(y) = \frac{(1+qy)^{\alpha}}{1-qy}, \quad |y| < q^{-1},$$

which has a zero $y = -q^{-1}$ with non-integral order $\alpha$.

Then we have

$$\begin{aligned} G(n) &= \frac{1}{2\pi i}\int_{|y|=r_1} \frac{(1+qy)^{\alpha}}{y^{n+1}(1-qy)}\,dy \\ &= \frac{q^n}{2\pi i}\int_{|z|=r} \frac{(1+z)^{\alpha}}{z^{n+1}(1-z)}\,dz, \end{aligned}$$

where $0 < r_1 < q^{-1}$ and $0 < r < 1$. Using the technique of contour integration, we can show that (cf. Zhang [6])

$$G(n) = q^n + O\left(q^n n^{-1-\alpha}\right).$$

For any $\gamma < 2$, we can choose $m$ sufficiently large, so that $1 + \alpha > \gamma$. Then (2.1) holds with $\gamma < 2$ and $Z(y)$ has a zero at $y = -q^{-1}$, with non-integral order $\alpha$.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Theorem 5.3.1, combined with Theorem 5.2.1, has the following direct consequence:

(5.3.4) COROLLARY. *If (2.1) holds with $\gamma > \frac{3}{2}$, then $Z(y)$ has either no zeros on the circle $|y| = q^{-1}$, or exactly one zero $y = -q^{-1}$, which then has order not exceeding one there. If (2.1) holds with $\gamma > 2$, then the only zero $y = -q^{-1}$ is of order one.*

*Proof.* Since $\alpha(\theta)$ is a non–negative integer for $0 < \theta < \frac{1}{2}$, (2.4) and (2.5) show that $\alpha(\theta) = 0$. Then the only possible zero is $y = -q^{-1}$, with order $\alpha\left(\frac{1}{2}\right) \leq 1$. If (2.1) holds with $\gamma > 2$, then $\alpha\left(\frac{1}{2}\right)$ is an integer, and hence $\alpha\left(\frac{1}{2}\right) = 0$ or 1. □

Next, Theorem 5.3.2, combined with Theorem 5.2.1, has the following direct consequence:

(5.3.5) COROLLARY. *If $f(z)$ satisfies all conditions of Theorem 5.3.2 with $\tau = 1$ and $\gamma > \frac{3}{2}$, then $f(z)$ has either no zeros on the circle $|z| = 1$ or exactly one zero $z = -1$, which is then of order not exceeding one there. If $\gamma > 2$, then the zero $z = -1$ is of order one.*

*Proof.* Since

$$\log f(z) = \sum_{k=1}^{\infty} c_k z^k, \quad |z| < 1,$$

with real coefficients $c_k \geq 0$, the McLaurin series of $f(z)$ has real coefficients. Hence the zeros of $f(z)$ are pairwise conjugate. We note that

$$\begin{aligned} \alpha(\theta) &= \sup\left\{\beta : (1-r)^{-\beta}\left|f(re^{2\pi i\theta})\right| \ll 1\right\} \\ &= \liminf_{r\to 1-} \frac{\log|f(re^{2\pi i\theta})|}{\log(1-r)}. \end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Therefore, a similar argument to the one given in the proof of Corollary 5.3.3 shows that the only possible zero is $z = -1$, with order $\alpha \leq 1$. If $\gamma > 2$, $\alpha$ is an integer, and hence $\alpha = 0$ or 1. □

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

## 5.4 An Alternative Abstract Prime Number Theorem

We can now give an answer to the fundamental question proposed in Section 5.2 (cf. Warlimont [1] and Zhang [7]).

(5.4.1) THEOREM. *If*

$$G(n) = Aq^n + O\left(q^n n^{-\gamma}\right) \tag{4.1}$$

*with* $A > 0$, $q > 1$, *and* $\gamma > 2$, *then either*

$$\bar{\Lambda}(n) = q^n\left(1 + O(n^{-\gamma+1})\right) \tag{4.2}$$

*or*

$$\bar{\Lambda}(n) = q^n\left(1 - (-1)^n + O(n^{-\gamma+2})\right). \tag{4.3}$$

*Remarks.* This theorem is a refinement of results of Warlimont [1] and Zhang [7]. The proof of (4.2) given below, due to Zhang, is published for the first time in this monograph, while the proof of (4.3), due to Warlimont, applies the same ideas as in the proofs of Theorem 5.5.1 and 5.5.4 below.

This theorem is essentially a variant of a tauberian theorem about the solution $\lambda(n)$ (*not* to be confused with the Liouville function $\lambda$ of classical number theory) to the convolution equation

$$\lambda * g(n) = ng(n), \quad n = 0, 1, 2, \ldots. \tag{4.4}$$

Thus, we shall first prove the following general tauberian theorem, and then Theorem 5.4.1 will follow directly.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

(5.4.2) THEOREM. *Let $\lambda(n)$ be arithmetical functions satisfying (4.4). If $\lambda(n) \geq 0$, $g(0) = 1$ and*

$$g(n) = A + O(n^{-\gamma}), \quad n \geq 1, \tag{4.5}$$

*with $A > 0$ and $\gamma > 2$, then either*

$$\lambda(n) = 1 + O\left(n^{-\gamma+1}\right) \tag{4.6}$$

*or*

$$\lambda(n) = 1 - (-1)^n + O\left(n^{-\gamma+2}\right). \tag{4.7}$$

*Proof.* Note, from (4.4), that $g(n) \geq 0$. Also note, from (4.5), that the generating function

$$\hat{G}(z) := \sum_{n=0}^{\infty} g(n) z^n \tag{4.8}$$

satisfies the conditions of Theorem 5.3.2 with $\tau = 1$ and $\gamma > 2$. Hence, by Corollary 5.3.5, $\hat{G}(z)$ has either no zeros on the circle $|z| = 1$ or exactly one zero $z = -1$, of order one there. We shall show that in the first case (4.6) holds, and in the second case (4.7) holds.

Thus we first assume that $\hat{G}(z) \neq 0$ on the circle $|z| = 1$. Let $V(z) := (1 - z)\hat{G}(z)$. Then $V(z) \neq 0$ on the closed disk $\{|z| \leq 1\}$. Note that

$$V(z) = 1 + \sum_{m=1}^{\infty} (g(m) - g(m-1)) z^m, \quad |z| \leq 1,$$

and

$$V'(z) = \sum_{m=1}^{\infty} m(g(m) - g(m-1)) z^{m-1}, \quad |z| \leq 1.$$

Let $\lambda(n) = 1 + r_n$. Then

$$\begin{aligned} r_n &= \frac{1}{2\pi i} \int_{|z|=1} \frac{V'(z)}{V(z)} \frac{dz}{z^n} = \frac{1}{2\pi} \int_{-\pi}^{\pi} \frac{V'(e^{i\theta})}{V(e^{i\theta})} e^{-i(n-1)\theta} d\theta \\ &= \frac{1}{2\pi} \sum_{m=1}^{\infty} m(g(m) - g(m-1)) \int_{-\pi}^{\pi} \frac{e^{i(m-n)\theta}}{V(e^{i\theta})} d\theta. \end{aligned} \tag{4.9}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

We need to show that $r_n = O(n^{-\gamma+1})$. Without loss of generality, we may assume $n > 3\gamma$. Let $k$ denote the greatest positive integer less than $\gamma - 1$. Then $V(z)$ has continuous derivatives of order $\leq k$ on $\{|z| \leq 1\}$. Let

$$I := \int_{-\pi}^{\pi} \frac{e^{i(m-n)\theta}}{V(e^{i\theta})}\, d\theta.$$

We claim that

$$I \ll |m-n|^{-k-1} \tag{4.10}$$

for $m \neq n$. This is certainly true for $m \in \{n-1, \ldots, n-2k+1\}$. Hence, we may assume that $m > n$ or $m \leq n - 2k$. By integration by parts, we obtain

$$\begin{aligned} I &= \frac{1}{m-n} \int_{-\pi}^{\pi} \frac{e^{i(m-n+1)\theta} V'(e^{i\theta})}{V^2(e^{i\theta})}\, d\theta \\ &= \frac{1}{m-n} \sum_{s=1}^{\infty} s(g(s) - g(s-1)) \int_{-\pi}^{\pi} \frac{e^{i(m+s-n)\theta}}{V^2(e^{i\theta})}\, d\theta. \end{aligned} \tag{4.11}$$

For $s \notin \{n-m, n-m-1, \ldots, n-m-k+1\}$, applying integration by parts $k$ times yields

$$\begin{aligned} \int_{-\pi}^{\pi} \frac{e^{i(m+s-n)\theta}}{V^2(e^{i\theta})}\, d\theta &= \frac{1}{(m+s-n)(m+s-n+1)\ldots(m+s-n+k-1)} \\ &\quad \times \int_{-\pi}^{\pi} \frac{P\left(V(e^{i\theta}), V'(e^{i\theta}), \ldots, V^{(k)}(e^{i\theta})\right)}{V^{k+2}(e^{i\theta})}\, d\theta \end{aligned}$$

where $P(x_0, x_1, \ldots, x_k)$ is a polynomial in $x_0, x_1, \ldots, x_k$ with integer coefficients, and hence

$$\int_{-\pi}^{\pi} \frac{e^{i(m+s-n)\theta}}{V^2(e^{i\theta})}\, d\theta \ll \frac{1}{|s+m-n|^k}. \tag{4.12}$$

From (4.11) and (4.12), if $m > n$, we obtain

$$I \ll \frac{1}{m-n} \sum_{s=1}^{\infty} \frac{s^{-\gamma+1}}{(s+m-n)^k} \ll \frac{1}{(m-n)^{k+1}}.$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

If $m \le n-2k$, we obtain

$$\begin{aligned} I &\ll \frac{1}{n-m}\left\{\sum_{1\le s\le n-m-k}\frac{s^{-\gamma+1}}{(n-m-s)^k}+\sum_{s\ge n-m+1}\frac{s^{-\gamma+1}}{(s+m-n)^k}\right. \\ &\qquad \left. +(n-m)^{-\gamma+1}+(n-m-1)^{-\gamma+1}+\cdots+(n-m-k+1)^{-\gamma+1}\right\} \\ &\ll (n-m)^{-\gamma}+\frac{1}{n-m}\left\{\sum_{1\le s\le n-m-k}\frac{s^{-\gamma+1}}{(n-m-s)^k}\right. \\ &\qquad \left. +\sum_{s\ge n-m+1}\frac{s^{-\gamma+1}}{(s+m-n)^k}\right\}. \end{aligned}$$

Note that $\frac{n-m-k}{2} \ge \frac{n-m}{4}$. Hence we have

$$\begin{aligned} \sum_{1\le s\le n-m-k}\frac{s^{-\gamma+1}}{(n-m-s)^k} &= \left(\sum_{1\le s<\frac{n-m-k}{2}}+\sum_{\frac{n-m-k}{2}\le s<n-m-k}\right)\frac{s^{-\gamma+1}}{(n-m-s)^k} \\ &\ll (n-m)^{-k}+(n-m)^{-\gamma+1}\log(n-m) \\ &\ll (n-m)^{-k}. \end{aligned}$$

Moreover,

$$\begin{aligned} \sum_{s\ge n-m+1}\frac{s^{-\gamma+1}}{(s+m-n)^k} &= \sum_{t=1}^{\infty}\frac{(t+n-m)^{-\gamma+1}}{t^k} \ll (n-m)^{-\gamma+1+\varepsilon}\sum_{t=1}^{\infty}\frac{1}{t^{k+\varepsilon}} \\ &\ll (n-m)^{-k}, \end{aligned}$$

if $\varepsilon>0$ and $\gamma-1-\varepsilon>k$. Therefore, if $m\le n-2k$, we also have

$$I \ll (n-m)^{-k-1}.$$

Now, from (4.9) and (4.10), we obtain

$$r_n \ll n^{-\gamma+1}+\sum_{\substack{m=1\\ m\ne n}}^{\infty}\frac{m^{-\gamma+1}}{|n-m|^{k+1}} \ll n^{-\gamma+1},$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

since

$$\begin{aligned}\sum_{m<n}\frac{m^{-\gamma+1}}{(n-m)^{k+1}} &= \left(\sum_{m<\frac{n}{2}}+\sum_{\frac{n}{2}\leq m<n}\right)\frac{m^{-\gamma+1}}{(n-m)^{k+1}}\\ &\ll n^{-k-1}+n^{-\gamma+1}\ll n^{-\gamma+1},\end{aligned}$$

and

$$\sum_{m>n}\frac{m^{-\gamma+1}}{(m-n)^{k+1}}\ll n^{-\gamma+1}.$$

This proves (4.6).

Next assume that $\hat{G}(-1)=0$. Let $\delta(n):=\lambda(n)-(1+(-1)^{n+1})$. Also, let

$$W(z):=\frac{1-z}{1+z}\hat{G}(z).$$

Then

$$W(z)=\frac{V(z)}{1+z}=\sum_{n=0}^{\infty}w(n)z^n.$$

Since $\hat{G}(-1)=0$, $V(-1)=0$ and we have

$$\begin{aligned}w(n) &= \sum_{k+m=n}(-1)^k(g(m)-g(m-1))\\ &= (-1)^n\sum_{m=0}^{n}(-1)^m(g(m)-g(m-1))\\ &= (-1)^{n+1}\sum_{m=n+1}^{\infty}(-1)^m(g(m)-g(m-1)),\end{aligned}$$

and hence $|w(n)|\ll n^{-\gamma+1}$, $n\geq 1$. Let

$$E(z):=W(z)W(-z)=\sum_{n=0}^{\infty}e(n)z^n,\quad |z|<1.$$

Then

$$e(n)=\sum_{j+k=n}w(j)(-1)^kw(k).$$

Note that

$$E(z) = \hat{G}(z)\hat{G}(-z) = \exp\left\{\sum_{k=1}^{\infty} \frac{\lambda(2k)}{k} z^{2k}\right\}, \quad |z| < 1.$$

Hence $e(n) \geq 0$ since $\lambda(n) \geq 0$. Let

$$(E(z))^{-1} = \sum_{n=0}^{\infty} d(n)z^n = \exp\left\{-\sum_{k=1}^{\infty} \frac{\lambda(2k)}{k} z^{2k}\right\}, \quad |z| < 1.$$

Then

$$|d(n)| \leq e(n) \leq \sum_{j+k=n} |w(j)|\,|w(k)| \ll n^{-\gamma+1}, \quad n \geq 1.$$

We now have,

$$\begin{aligned}\sum_{n=0}^{\infty} \delta(n)z^n &= \frac{z\hat{G}'(z)}{\hat{G}(z)} - \frac{1}{1-z} + \frac{1}{1+z} \\ &= \frac{zW'(z)}{W(z)} = zW'(z)(E(z))^{-1}W(-z),\end{aligned}$$

and then

$$\delta(n) = \sum_{\substack{m+h+\ell=n \\ h,\ell\geq 0,\, m\geq 1}} mw(m)d(h)(-1)^{\ell}w(\ell).$$

Therefore

$$\begin{aligned}\delta(n) &\ll n\left(\sum_{\substack{m+h+\ell=n \\ m,h,\ell\geq 1}} m^{-\gamma+1}h^{-\gamma+1}\ell^{-\gamma+1} + \sum_{\substack{m+\ell=n \\ m,\ell\geq 1}} m^{-\gamma+1}\ell^{-\gamma+1} + n^{-\gamma+1}\right) \\ &\ll n^{-\gamma+2}.\end{aligned}$$

This proves (4.7). □

*Proof of Theorem 5.4.1* We have

$$\bar{\Lambda} * G(n) = nG(n), \quad n = 0, 1, 2, \ldots .$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Let $\bar{\Lambda}(n) = q^n\lambda(n)$ and $G(n) = q^n g(n)$. Then $\lambda(n)$ and $g(n)$ satisfy the conditions of Theorem 5.4.2. Thus (4.2) and (4.3) follow from (4.6) and (4.7). □

We may also consider an elementary proof of the above alternative abstract prime number theorem. The question of an elementary proof was also proposed by Bombieri [2] in a different form, in relation with Bombieri's tauberian theorem given in Section 3.6 of Chapter 3. An answer to Bombieri's question was given by A. Granville in [1]. A. Hildebrand and G. Tenenbaum [1] considered a similar problem in more general form, and proved the following theorem. However, their proof is not elementary, and will not be treated here.

(5.4.3) THEOREM. *Suppose $\{a_n\}_{n=1}^{\infty}$ is a sequence of non-negative real numbers satisfying*

$$na_n + \sum_{k=1}^{n-1} a_k a_{n-k} = 2n + O(R(n)), \quad n \geq 1,$$

*where $R(n)$ is a positive-valued function with the properties: (1) $R(n)$ is non-decreasing, (2) $R(n)/n$ is non-increasing, and (3) $\lim_{n\to\infty} R(n)/n = 0$. Then either*

$$a_n = 1 + O\left(\frac{R(n)}{n}\right), \quad n \geq 1$$

*or*

$$a_n = 1 + (-1)^{n+1} + O\left(\frac{R(n)}{n}\right), \quad n \geq 1.$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

## 5.5 Beurling–Type Abstract Prime Number Theorems

Another class of abstract prime number theorems which are not of classical type consists of *"Beurling–type"* abstract prime number theorems. In this section, we shall give a brief *survey* of some Beurling–type abstract prime number theorems, without involving any proofs. (Readers interested in the proofs may read Warlimont [1] and Zhang [2,6,7], in particular.)

While investigating the proof of the classical prime number theorem, Beurling [1] (cf. also Bateman and Diamond [1]) suggested the consideration of the following general situation:

Let $\mathcal{P}$ be a sequence $\{p_1, p_2, \ldots\}$ of positive real numbers such that

$$1 < p_1 \leq p_2 \leq \cdots, \quad p_j \to \infty \text{ as } j \to \infty;$$

which is called, following Beurling, a sequence of *generalized primes.* The multiplicative semigroup $\mathcal{G}$ generated by $\mathcal{P}$ is countable and may be arranged in a non–decreasing sequence

$$n_0 = 1 < n_1 \leq n_2 \leq \cdots,$$

which is called the sequence of *generalized integers* associated with $\mathcal{P}$.

Based on this suggestive (but slightly deceptive) nomenclature, Beurling [1] and others (see e.g. also Bateman and Diamond [1], Diamond [1–4], R.S. Hall [1,2], Müller [1,2] and Ryavec [1]) raised and answered various analytical questions in parallel to the asymptotic counting problems of classical prime number theory in $\mathbb{N}$, some of which will be described shortly.

*Warning Remark.* Without questioning the soundness of the main analytical conclusions of these authors, readers should however be warned that

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

in *some* of the cited literature there is a deceptive looseness or incompleteness of description of the initial concepts involved, which should at least be clarified: The source of this imprecision lies in a frequent failure to distinguish between $\mathcal{P}$ and $\mathcal{G}$ as *sets* of real numbers rather than as *sequences*. Thus generalized primes or integers which are distinct as sequence elements are allowed to have the same real value, and generalized integers $n_i$ and $n_j$ of possibly equal value should nevertheless be distinguished if they arise from distinct formal products of generalized primes. In actual fact the authors of papers on "generalized" or "Beurling" numbers often *implicitly* deal with an arithmetical semigroup $\mathcal{G}_0$, with prime set $\mathcal{P}_0$ and a not necessarily integer–valued norm mapping $|\ |$, and then (sometimes loosely) identifying $\mathcal{P}_0$ and $\mathcal{G}_0$ with the image sets $\mathcal{P} = |\mathcal{P}_0|$ and $\mathcal{G} = |\mathcal{G}_0|$.

Taking the above comments as understood we now turn to the asymptotic analysis of suitable counting functions associated with $\mathcal{G}$, $\mathcal{P}$: Let

$$N(x) = \sum_{\substack{i \\ n_i \leq x}} 1, \quad \psi(x) = \sum_{\substack{i,k \\ p_i^k \leq x}} \log p_i;$$

denote the basic counting function of generalized integers, and the counterpart of the Chebyshev function in classical number theory, respectively. Beurling showed that if

$$N(x) = Ax + O\left(x \log^{-\gamma} x\right) \tag{5.1}$$

with positive constant $A$ and $\gamma > \frac{3}{2}$ then

$$\psi(x) \sim x \text{ as } x \to \infty, \tag{5.2}$$

which is a counterpart of the prime number theorem for $\mathbb{N}$. He also showed, by examples, that if $\gamma = \frac{3}{2}$ in (5.1), then the prime number theorem need not hold. Beurling investigated also the more general case in which

$$N(x) = x \sum_{\nu=1}^{n} A_\nu \log^{\rho_\nu - 1} x + O\left(x \log^{-\gamma} x\right), \tag{5.3}$$

where $\rho_1 < \rho_2 < \cdots < \rho_n$ and $A_1, A_2, \ldots, A_n$ are arbitrary real numbers. He showed that if (5.3) holds with $1 \leq \rho_n = \tau < 2$ for some $A_n > 0$ and $\gamma > 1 + \frac{\tau}{2}$ then $\psi(x) \sim \tau x$, a generalization of the prime number theorem. However, if $\tau \geq 2$, even an $O(1)$–error term in (5.3) does not guarantee $\psi(x) \sim \tau x$. Still Beurling proved that, if (5.3) holds with $\rho_n = \tau \geq 2$ for some $A_n > 0$ and $\gamma > 1 + \frac{\tau}{2}$, then there exist $0 < t_1 \leq t_2 \leq \cdots \leq t_q < \infty$ with $q \leq [\tau/2]$ such that

$$\psi(x) \sim x \left\{ \tau - 2 \sum_{\nu=1}^{q} \cos\left(t_\nu \log x - \ \arctan\, t_\nu\right) \right\}$$

as $x \to \infty$.

We can also consider abstract prime number theorems and Chebyshev–type upper bounds on *additive* arithmetical semigroups which satisfy a "Beurling–type" condition of the form

$$G(n) = q^n \sum_{\nu=1}^{r} a_\nu n^{\rho_\nu - 1} + O\left(q^n n^{-\gamma}\right), \tag{5.4}$$

or

$$G(n) = q^n \sum_{\nu=1}^{r} a_\nu n^{\rho_\nu - 1} + O\left(q^{vn}\right), \tag{5.5}$$

where $\rho_1 < \rho_2 < \cdots < \rho_r$ and $A_1, A_2, \ldots, A_r$ are arbitrary real numbers such that $q > 1$, $\rho_r > 0$, $A_r > 0$, $0 \leq v < 1$, and $\gamma > 1$. In this case, a generalization of the abstract prime number theorem (henceforth, *P.N.T.*) states that $P(n) \sim \rho_r q^n n^{-1}$, or (equivalently) $\bar{\Lambda}(n) \sim \rho_r q^n$, as $n \to \infty$.

### 5.5.1 Chebyshev–type upper bounds (cf. Zhang [2])

(5.5.1) THEOREM. *Suppose that*

$$\sum_{n=1}^{\infty} \sup_{n \leq n} \left| G(m) q^{-m} - \sum_{\nu=1}^{r} A_\nu m^{\rho_\nu - 1} \right| < \infty, \tag{5.6}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

*and $\rho_r \geq 1$. Then $\bar{\Lambda}(n) \ll q^n$. Moreover, if $\rho_1 > 0$, then*

$$\sum_{m=1}^{n} \frac{\bar{\Lambda}(m)}{q^m} = \rho_r n + R(n) + O(1), \tag{5.7}$$

*where $R(n)$ is an elementary function of $n$ with $R(n) \ll n^{\alpha}$ for some $\alpha < 1$.*

*Remark.* This function $R(n)$ is a sum of a finite number of terms of the form

$$an^{-k\rho_r + L(\rho)+1-\ell}. \tag{5.8}$$

Here $k \in \mathbb{N}$, $\ell \in \mathbb{N} \cup \{0\}$, $\rho = (\rho_1, \dots, \rho_r)$ and $L(\rho)$ is a linear function of $\rho_1, \dots, \rho_{r-1}$ and $\ell_\nu - \ell$, $\ell \in \mathbb{N}$, $\ell \leq [\rho_\nu]$, $\nu = 1, 2, \dots, r$. The coefficients of $L(\rho)$ are non-negative integers and their sum is $k$. the coefficient $a$ in (5.8) is an explicit rational function of $\rho_1, \dots, \rho_r$ and $A_1, \dots, A_r$. In particular,

$$R(n) = \begin{cases} O(1), & \text{if } r = 1, \\ O\left(1 + n^{\rho_{r-1}+1-\rho_r}\right), & \text{if } r \geq 2. \end{cases} \tag{5.9}$$

On the basis of Theorem 5.5.1, we can (cf. Zhang [8]) prove mean value theorems of multiplicative functions on additive arithmetical semigroups which are analogues of the Halász theorem, the Halász–Wirsing theorem, and the Halász–Wirsing–Delange theorem in classical probabilistic number theory, respectively. (Also, see Chapter 6 below.)

(5.5.2) Corollary. *If*

$$G(n) = q^n \sum_{\nu=1}^{r} A_\nu n^{\rho_\nu - 1} + O\left(q^n n^{-\gamma}\right)$$

*with $\gamma > 1$, then $\bar{\Lambda}(n) \ll q^n$, and (5.7) holds.*

On the basis of Corollary 5.5.2, an analogue of the Erdős–Wintner theorem can be proved for additive arithmetical semigroups (cf. Zhang [3]).

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

### 5.5.2 Beurling–type abstract prime number theorems (cf. Warlimont [1] and Zhang [6])

The following theorem contains a complete answer to the question about the relation between Beurling–type abstract prime number theorems "close to classical sense" and zeros of the generating function $Z(y)$ on the circle $|y| = q^{-1}$.

(5.5.3) THEOREM. *Assume (5.4) with $\gamma > 1$. Then $\bar{\Lambda}(n) \sim \rho_\tau q^n$ if and only if $Z(y) \neq 0$ on the circle $|y| = q^{-1}$.*

The next theorem about the "total number" of zeros of the generating function $Z(y)$ on the circle $|y| = q^{-1}$ is a generalization of Theorem 5.2.1, under the condition (5.4) with $\gamma > 1$. It is a direct consequence of Theorem 5.2.2.

(5.5.4) THEOREM. *Suppose that (5.4) holds with $\gamma > 1$. Then the "total number" of zeros of $Z(y)$ on the circle $|y| = q^{-1}$ is at most $\tau = \rho_\tau$, in the sense that*

$$\alpha\left(\frac{1}{2}\right) + 2 \sum_{0<\theta<\frac{1}{2}} \alpha(\theta) \leq \tau,$$

*or*

$$2 \sum_{0<\theta<\frac{1}{2}} \alpha(\theta) \leq \tau,$$

*according as $-q^{-1}$ is or is not a zero of $Z(y)$, where the summation is taken over all zeros of $Z(y)$ on the upper half of the circle $|y| = q^{-1}$.*

If we strengthen the condition (5.4) with $\gamma > 1$ slightly, then the order of a zero of $Z(y)$ will be a positive integer:

(5.5.5) THEOREM. *Let $q^{-1}e^{2\pi i\theta}$ be a zero of $Z(y)$, with order $\alpha = \alpha(\theta)$ where $0 < \theta < 1$.*

*(1) If (5.4) holds with $\gamma > 1$, then $\alpha \geq \min\{1, \gamma - 1\}$.*

*(2) If (5.4) holds with $\gamma > 1 + \alpha$, in particular, if $\theta \neq \frac{1}{2}$ and (5.4) holds with $\gamma > 1 + \frac{\tau}{2}$ or if $\theta = \frac{1}{2}$ and (5.4) holds with $\gamma > 1 + \tau$, then $\alpha$ is a positive integer.*

*Moreover, if (5.4) holds with $\gamma > 1 + \alpha$, then*

$$\lim_{r \to q^{-1}-} \frac{Z(re^{2\pi i\theta})}{\left(q^{-1} - r\right)^{\alpha} e^{2\pi i\alpha\theta}} = \frac{(-1)^{\alpha}}{\alpha!} Z^{(\alpha)} \left(q^{-1}e^{2\pi i\theta}\right) \neq 0,$$

*and $Z(y)/\left(q^{-1}e^{2\pi i\theta} - y\right)^{\alpha}$ is continuous on $\{y : |y| \leq q^{-1}, |y - q^{-1}e^{2\pi i\theta}| < \varepsilon\}$, for some $\varepsilon > 0$.*

Next, in the case $\tau = \rho_r < 1$, we have an abstract prime number theorem "close to the classical sense":

(5.5.6) THEOREM. *If (5.4) holds with $0 < \tau = \rho_r < 1$, and $\gamma > 1 + \tau$, then $\bar{\Lambda}(n) \sim \tau q^n$.*

This last theorem can fail if $\tau = \rho_r > 1$:

(5.5.7) THEOREM. *For $\tau = \rho_r > 1$, the hypothesis*

$$G(n) = q^n \sum_{\nu=1}^{r} A_\nu n^{\rho_\nu - 1}$$

*does not generally entail $\bar{\Lambda}(n) \sim \tau q^n$. However for $\tau \geq 1$:*

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

(1) *If the condition (5.4) holds with $\gamma > 1 + \tau$, then there exist a non-negative integer $k$ with $k \leq (\tau + 1)/2$, $k$ real numbers $\theta_1, \ldots, \theta_k$ with $0 < \theta_1 < \cdots < \theta_k \leq \frac{1}{2}$, and $k$ positive integers $n_1, \ldots, n_k$, such that*

$$\bar{\Lambda}(n) = q^n \left( \tau - 2 \sum_{\nu=1}^{k-1} n_\nu \cos 2n\pi\theta_\nu - (-1)^n n_k + o(1) \right), \tag{5.10}$$

*and*

$$n_k + 2 \sum_{\nu=1}^{k-1} n_\nu \leq [\tau] \quad \textit{if} \quad \theta_k = \frac{1}{2}, \tag{5.11}$$

*or such that*

$$\bar{\Lambda}(n) = q^n \left( \tau - 2 \sum_{\nu=1}^{k} n_\nu \cos 2n\pi\theta_\nu + o(1) \right), \tag{5.12}$$

*and*

$$2 \sum_{\nu=1}^{k} n_\nu \leq [\tau] \quad \textit{if} \quad \theta_k < \frac{1}{2}. \tag{5.13}$$

(2) *If the generating function $Z(y)$ has no zero at $y = -q^{-1}$, and (5.4) holds with $\gamma > 1 + \frac{\tau}{2}$, then (5.12) and (5.13) hold with $k \leq \tau/2$. In particular, if $\tau < 2$ and $Z\left(-q^{-1}\right) \neq 0$, then $\bar{\Lambda}(n) = q^n(\tau + o(1))$.*

The first part of Theorem 5.5.7 is shown by two examples in Zhang [6].

### 5.5.3 Remainder estimates (cf. Zhang [7])

In Theorems 5.5.6 and 5.5.7, the remainders are of $o(1)$ form. In applications, a better estimate of the remainder than $o(1)$ is required. This estimate has been given in case $G(n) = Aq^n + O\left(q^n n^{-\gamma}\right)$ with $\gamma > 2$ in Theorem 5.4.1. It sounds best possible in some sense. In the general case, we have the following theorem. Here it seems possible to relax the condition $\gamma > \max\{2+\rho_r, 3\}$ in the theorem to $\gamma > \max\{1+\rho_r, 2\}$.

Let $[a]_1$ denote the greatest integer less than $a$. Also, as usual, let $[a]$ denote the greatest integer less than or equal to $a$. Thus $[a]_1 = [a]-1$ or $[a]_1 = [a]$ according as $a$ is or is not an integer. Let $R_1$ denote the set of $\rho_j$ which are positive integers, $R_2$ denote the set of $\rho_j$ which are 0 or negative integers, and $R_3$ the set of $\rho_j$ which are non–integers. Set

$$m_1 := \min\{[\rho_r - \rho_j],\ \rho_j \in (R_1 \cup R_3) - \{\rho_r\}\} \tag{5.14}$$

if $(R_1 \cup R_3) - \{\rho_r\}$ is not empty. Also, set

$$m_2 := \begin{cases} [\rho_r]_1, & \text{if some } \rho_j = 0; \\ [\gamma]_1 - 1, & \text{if } R_2 = \emptyset \text{ and if } \rho_r \text{ is an integer;} \\ [\rho_r], & \text{else.} \end{cases} \tag{5.15}$$

(5.5.8) THEOREM. *Assume (5.4) with $q > 1$ and $\gamma > \max\{2+\rho_r, 3\}$. Then there exist some constant $\sigma_0 > 0$, $k$ real numbers $0 < \theta_1 < \cdots < \theta_k \le \frac{1}{2}$, and $k$ positive integers $n_1, \ldots, n_k$ such that*

$$\bar{\Lambda}(n) = q^n\left(\rho_r - 2\sum_{\ell=1}^{k-1} n_\ell \cos 2n\pi\theta_\ell - (-1)^n n_k\right) + O\left(q^n n^{-t-\sigma}\right) \tag{5.16}$$

*and*

$$n_k + 2\sum_{\ell=1}^{k-1} n_\ell \le \rho_r \tag{5.17}$$

*if $\theta_k = \frac{1}{2}$ or such that*

$$\bar{\Lambda}(n) = q^n\left(\rho_r - 2\sum_{\ell=1}^{k} n_\ell \cos 2n\pi\theta_\ell\right) + O\left(q^n n^{-t-\sigma}\right) \tag{5.18}$$

*and*

$$2\sum_{\ell=1}^{k} n_\ell \le \rho_r \tag{5.19}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

*if* $\theta_k < \frac{1}{2}$. *Here the non–negative integer* $k \leq (\rho_r + 1)/2$ *and* $\sigma$ *is any constant satisfying* $0 < \sigma < \sigma_0$. *Also,*

$$t := \min\{m_1, m_2, m_3, [\gamma]_1 - 3\} \tag{5.20}$$

*with*

$$m_3 := \begin{cases} [\gamma]_1 - 1 - \max\{n_1, \ldots, n_k\}, & \textit{if } k \geq 1, \\ [\gamma]_1 - 1, & \textit{if } k = 0 \end{cases} \tag{5.21}$$

*if* $(R_1 \cup R_3) = \{\rho_r\}$ *is not empty and if* $\rho_r - \rho_j$ *are not all positive integers for* $\rho_j \in (R_1 \cup R_3) - \{\rho_r\}$ *and*

$$t := \min\{m_2, m_3, [\gamma]_1 - 3\} \tag{5.22}$$

*otherwise.*

*Remark.* For effective computation of the value of constant $\sigma_0$, see Zhang [7].

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

# CHAPTER 6

# GENERAL MEAN–VALUE THEOREMS

In this chapter we study the mean–value properties of complex–valued *multiplicative* functions $f$ satisfying $|f(a)| \leq 1$ for all $a$ in an (additive) arithmetical semigroup $\mathcal{G}$. Thus we study the asymptotic properties of the summatory function

$$F(n) := \bar{f}(n) = \sum_{\partial(a)=n} f(a), \text{ as } n \to \infty.$$

The generating function of $F$ and $f$ is

$$\begin{aligned} \hat{F}(y) : &= \sum_{n=0}^{\infty} F(n) y^n = \sum_{a \in \mathcal{G}} f(a) y^{\partial(a)} = f^{\#}(y) \\ &= \prod_{p \in \mathcal{P}} \left(1 + \sum_{k=1}^{\infty} f(p^k) y^{k\partial(p)}\right), \end{aligned} \qquad (0.1)$$

by Lemma 1.4.1.

Several authors have made contributions to this subject (e.g. Indlekofer and Manstavicius [1], Warlimont [4], and Zhang [8]). The discussion given here follows mainly the paper [8] of Zhang.

## 6.1 Preliminaries

We first prepare the ground for the proofs of mean–value theorems by introducing preliminary estimates and convolution techniques.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

### 6.1.1 Preliminary estimates

(6.1.1) LEMMA. *Let $\hat{G}_k(z) := \sum_{n=0}^{\infty} c_{k,n} z^n$, $k = 1, 2$, converge for $|z| < R$. Suppose that $|c_{1,n}| \leq c_{2,n}$, $n = 0, 1, 2, \ldots$ . Then for $0 < \eta \leq \pi$ and $0 < r < R$ we have*

$$\int_{\theta_0}^{\theta_0+\eta} \left|\hat{G}_1(re^{i\theta})\right|^2 d\theta \leq 2\int_{-\eta}^{\eta} \left|\hat{G}_2(re^{i\theta})\right|^2 d\theta.$$

PROOF. We have

$$\frac{1}{\eta}\int_{-\eta}^{\eta} \left(1 - \frac{|\theta|}{\eta}\right) e^{ix\theta} d\theta = \begin{cases} \left(\dfrac{\sin\left(\frac{\eta x}{2}\right)}{\frac{\eta x}{2}}\right)^2, & \text{for } x \neq 0, \\ 1, & \text{for } x = 0. \end{cases}$$

Therefore, for $0 < r < R$, we have

$$\begin{aligned} &\int_{\theta_0}^{\theta_0+\eta} \left|\hat{G}_1(re^{i\theta})\right|^2 d\theta \\ &\quad = \int_{-\frac{\eta}{2}}^{\frac{\eta}{2}} \left|\hat{G}_1\left(re^{i\left(\theta_0+\frac{\eta}{2}+\theta\right)}\right)\right|^2 d\theta \\ &\quad \leq 2\int_{-\eta}^{\eta} \left(1 - \frac{|\theta|}{\eta}\right) \left|\hat{G}_1\left(re^{i\left(\theta_0+\frac{\eta}{2}+\theta\right)}\right)\right|^2 d\theta \\ &\quad = 2\sum_{n,m=0}^{\infty} c_{1,n}\bar{c}_{1,m} r^{n+m} \int_{-\eta}^{\eta} \left(1 - \frac{|\theta|}{\eta}\right) e^{i(n-m)\left(\theta_0+\frac{\eta}{2}+\theta\right)} d\theta \\ &\quad \leq 2\sum_{n,m=0}^{\infty} c_{2,n} c_{2,m} r^{n+m} \int_{-\eta}^{\eta} \left(1 - \frac{|\theta|}{\eta}\right) e^{i(n-m)\theta} d\theta \\ &\quad = 2\int_{-\eta}^{\eta} \left(1 - \frac{|\theta|}{\eta}\right) \left|\hat{G}_2(re^{i\theta})\right|^2 d\theta \\ &\quad \leq 2\int_{-\eta}^{\eta} \left|\hat{G}_2(re^{i\theta})\right|^2 d\theta. \qquad \square \end{aligned}$$

Let

$$T(z) := \hat{F}\left(q^{-1}z\right).$$

For simplicity of computation, we shall use $T(z)$ instead of $\hat{F}(y)$ in the proofs of mean–value theorems in the following sections. Thus we begin with an analysis of $T(z)$.

(6.1.2) LEMMA. *Assume $G(n) \ll q^n$ with $q > 1$. Let $f$ be a multiplicative function such that $|f(a)| \leq 1$ for all $a \in \mathcal{G}$. If for each $p \in \mathcal{P}$ with $\partial(p) < \frac{\log 2}{\log q}$ there exists a positive integer $k(p)$ such that $q^{\partial(p)} - 1 - q^{-\partial(p)\left(k(p)-1\right)} \geq 0$, and such that $f(p^k) = 0$ for all $1 \leq k < k(p)$, then, for $|z| < 1$, $T(z) \neq 0$ and*

$$T(z) = T_1(z)T_2(z)T_3(z), \tag{1.1}$$

*where*

$$T_1(z) := \prod_{\partial(p)<\frac{\log 3}{\log q}} \left(1 + \sum_{k=1}^{\infty} f(p^k)(q^{-1}z)^{k\partial(p)}\right) \tag{1.2}$$

*is holomorphic in the disk $\{|z| < q\}$,*

$$T_2(z) := \prod_{\partial(p)\geq\frac{\log 3}{\log q}} \left(1 - f(p)(q^{-1}z)^{\partial(p)}\right)^{-1} \tag{1.3}$$

*is holomorphic in the disk $\{|z| < 1\}$, and*

$$T_3(z) := \prod_{\partial(p)\geq\frac{\log 3}{\log q}} \left(1 + \sum_{k=2}^{\infty} \left(f(p^k) - f(p^{k-1})f(p)\right)(q^{-1}z)^{k\partial(p)}\right) \tag{1.4}$$

*is holomorphic in the disk $\{|z| < q^{1/2}\}$.*

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Proof. For $|z| < 1$, we have

$$\begin{aligned}\sum_{a\in\mathcal{G}} |f(a)|\,|q^{-1}z|^{\partial(a)} &\leq \sum_{m=0}^{\infty} G(m)\left(q^{-1}|z|\right)^{m}\\ &\ll \sum_{m=0}^{\infty} |z|^{m} < \infty.\end{aligned}$$

Hence $T(z)$ is holomorphic in the disk $\{|z| < 1\}$, and the canonical (Euler-type) product formula

$$T(z) = \prod_{p}\left(1 + \sum_{k=1}^{\infty} f(p^{k})(q^{-1}z)^{k\partial(p)}\right)$$

holds there. It follows that $T(z) \neq 0$ for $|z| < 1$, since

$$\begin{aligned}\left|1 + \sum_{k=1}^{\infty} f(p^{k})(q^{-1}z)^{k\partial(p)}\right| &\geq 1 - \sum_{k=1}^{\infty}\left(q^{-1}|z|\right)^{k\partial(p)}\\ &= \frac{1 - 2\left(q^{-1}|z|\right)^{\partial(p)}}{1 - \left(q^{-1}|z|\right)^{\partial(p)}} > 0 \qquad (1.5)\end{aligned}$$

for $p$ with $\partial(p) \geq \frac{\log 2}{\log q}$, and

$$\begin{aligned}\left|1 + \sum_{k=1}^{\infty} f(p^{k})(q^{-1}z)^{k\partial(p)}\right| &\geq 1 - \sum_{k=k(p)}^{\infty}\left(q^{-1}|z|\right)^{k\partial(p)}\\ &= \frac{1 - \left(q^{-1}|z|\right)^{\partial(p)} - \left(q^{-1}|z|\right)^{k(p)\partial(p)}}{1 - \left(q^{-1}|z|\right)^{\partial(p)}}\\ &> 0 \qquad (1.6)\end{aligned}$$

for $p$ with $\partial(p) < \frac{\log 2}{\log q}$.

Then, for $|z| < 1$,

$$\begin{aligned}&\sum_{\partial(p)\geq\frac{\log 3}{\log q}}\sum_{k=1}^{\infty}\left|f^{k}(p)\left(q^{-1}z\right)^{k\partial(p)}\right|\\ &\qquad \leq \sum_{m=0}^{\infty} G(m)\left(q^{-1}|z|\right)^{m} < \infty.\end{aligned}$$

Hence the infinite product (1.3) converges absolutely, and $T_2(z)$ is holomorphic in the disk $\{|z| < 1\}$.

We now consider the infinite product (1.4). For $|z| < q^{1/2}$, we have

$$\begin{aligned}
&\sum_{\partial(p)\ge\frac{\log 3}{\log q}} \sum_{k=2}^{\infty} \left| \left( f(p^k) - f(p^{k-1}) f(p) \right) (q^{-1}z)^{k\partial(p)} \right| \\
&\quad \le \sum_{\partial(p)\ge\frac{\log 3}{\log q}} \frac{2\left(q^{-1}|z|\right)^{2\partial(p)}}{1-3^{-1/2}} \ll \sum_{m=0}^{\infty} G(m) q^{-2m} |z|^{2m} \\
&\quad < \infty.
\end{aligned}$$

Hence the infinite product (1.4) converges absolutely for $|z| < q^{1/2}$, and thus $T_3(z)$ is holomorphic in the disk $\{|z| < q^{1/2}\}$.

Finally, we have

$$\begin{aligned}
&\left(1 + \sum_{k=1}^{\infty} f(p^k)(q^{-1}z)^{k\partial(p)}\right) \left(1 - f(p)(q^{-1}z)^{\partial(p)}\right) \\
&\qquad = 1 + \sum_{k=2}^{\infty} \left( f(p^k) - f(p^{k-1}) f(p) \right) (q^{-1}z)^{k\partial(p)}
\end{aligned}$$

for $|z| < q$, and (1.1) follows. □

(6.1.3) LEMMA. *Suppose that*

$$\sum_{n=1}^{\infty} \left| G(n) q^{-n} - A \right| < \infty, \tag{1.7}$$

*and either*

$$G(n) q^{-n} - A = O(n^{-1}) \tag{1.8}$$

*or*

$$\sum_{n=1}^{\infty} n \left( G(n) q^{-n} - A \right)^2 < \infty. \tag{1.9}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

*Let $f$ be a completely multiplicative function such that $|f(a)| \leq 1$ for all $a \in \mathcal{G}$. Then, for $0 \leq r < 1$,*

$$\int_{-\pi}^{\pi} \left| \frac{re^{i\theta}T'(re^{i\theta})}{T(re^{i\theta})} \right|^2 d\theta \ll \frac{1}{1-r}. \tag{1.10}$$

PROOF. Since $f$ is completely multiplicative, we have

$$\frac{zT'(z)}{T(z)} = \sum_p \sum_{k=1}^{\infty} \partial(p) f^k(p) (q^{-1}z)^{k\partial(p)}.$$

Note that

$$\frac{q^{-1}zZ'(q^{-1}z)}{Z(q^{-1}z)} = \sum_p \sum_{k=1}^{\infty} \partial(p)(q^{-1}z)^{k\partial(p)}.$$

Hence, by Lemma 6.1.1,

$$\int_{\theta_0}^{\theta_0+\eta} \left| \frac{re^{i\theta}T'(re^{i\theta})}{T(re^{i\theta})} \right|^2 d\theta \leq 2 \int_{-\eta}^{\eta} \left| \frac{q^{-1}re^{i\theta}Z'(q^{-1}re^{i\theta})}{Z(q^{-1}re^{i\theta})} \right|^2 d\theta. \tag{1.11}$$

We need now a suitable choice of $\eta$:

From (1.7), we have

$$Z(y) = \frac{1}{1-qy}[A + (1-qy)R(y)],$$

where

$$R(y) = 1 - A + \sum_{m=1}^{\infty} \left( G(m)q^{-m} - A \right) (qy)^m$$

is continuous on the closed disk $\{|y| \leq q^{-1}\}$. Note that $Z(y)$ has no zeros in the open disk $\{|y| < q^{-1}\}$. Hence there exists a number $\eta > 0$ such that $A + (1-qy)R(y) \neq 0$ for $y = re^{i\theta}$ with $0 \leq r \leq q^{-1}$, $|\theta| \leq \eta$, since $A > 0$. We now fix $0 < \eta < \pi$. Then we have, for $|z| < 1$,

$$\frac{q^{-1}zZ'(q^{-1}z)}{Z(q^{-1}z)} = \frac{z}{1-z} + \frac{-zR(q^{-1}z) + q^{-1}z(1-z)R'(q^{-1}z)}{A + (1-z)R(q^{-1}z)}.$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

It follows that

$$\int_{-\eta}^{\eta}\left|\frac{re^{i\theta}Z'(q^{-1}re^{i\theta})}{Z(q^{-1}re^{i\theta})}\right|^2 d\theta$$
$$\ll 1+\int_{-\eta}^{\eta}\left(\frac{1}{|1-re^{i\theta}|^2}+\left|R'(q^{-1}re^{i\theta})\right|^2\right)d\theta.$$

We have

$$\int_{-\eta}^{\eta}\frac{1}{|1-re^{i\theta}|^2}d\theta \le \int_{-\pi}^{\pi}\frac{d\theta}{|1-re^{i\theta}|^2}=\frac{2\pi}{1-r^2}\ll\frac{1}{1-r},$$

by the Poisson integral formula (cf. Titchmarsh [1]). Also, we have

$$\int_{-\pi}^{\pi}\left|R'(q^{-1}re^{i\theta})\right|^2 d\theta = 2\pi\sum_{m=1}^{\infty}m^2\left(G(m)q^{-m}-A\right)^2 r^{2m-2}.$$

If we assume (1.8), then plainly

$$\sum_{m=1}^{\infty}m^2\left(G(m)q^{-m}-A\right)^2 r^{2m}\ll\sum_{m=1}^{\infty}r^{2m}\ll\frac{1}{1-r}.$$

If we assume (1.9), letting $S_0=0$ and

$$S_n:=\sum_{m=1}^{n}m\left(G(m)q^{-m}-A\right)^2,\quad n\ge 1,$$

then, by summation by parts, we have

$$\begin{aligned}\sum_{n=1}^{\infty}n^2\left(G(n)q^{-n}-A\right)^2 r^{2n}&=\sum_{n=1}^{\infty}n(S_n-S_{n-1})r^{2n}\\&=(1-r^2)\sum_{n=1}^{\infty}(n+1)S_nr^{2n}-\sum_{n=1}^{\infty}S_nr^{2n}\\&\ll(1-r^2)\sum_{n=1}^{\infty}(n+1)r^{2n}=(1-r^2)\left(\frac{1}{(1-r)^2}-1\right)\\&\ll\frac{1}{1-r}.\end{aligned}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Thus we obtain
$$\int_{-\eta}^{\eta} \left| \frac{re^{i\theta} Z'(q^{-1}re^{i\theta})}{Z(q^{-1}re^{i\theta})} \right|^2 d\theta \ll \frac{1}{1-r}, \tag{1.12}$$
and then (1.10) follows from (1.11) and (1.12). □

(6.1.4) Lemma. *Assume that (1.7) and either (1.8) or (1.9) hold. If $f$ satisfies the conditions of Lemma 6.1.2, then for $0 \le r < 1$, (1.10) hold too.*

Proof. By Lemma 6.1.2, for $0 \le r < 1$, we have
$$\frac{T'(re^{i\theta})}{T(re^{i\theta})} = \frac{T_1'(re^{i\theta})}{T_1(re^{i\theta})} + \frac{T_2'(re^{i\theta})}{T_2(re^{i\theta})} + \frac{T_3'(re^{i\theta})}{T_3(re^{i\theta})},$$
and
$$\int_{-\pi}^{\pi} \left| \frac{re^{i\theta} T_3'(re^{i\theta})}{T_3(re^{i\theta})} \right|^2 d\theta \ll 1, \tag{1.13}$$
since $1 \ll |T_3(z)| \ll 1$ and $|T_3'(z)| \ll 1$ in the disk $\{|z| \le 1\}$. Then, note that
$$\frac{zT_2'(z)}{T_2(z)} = \sum_{\partial(p) \ge \frac{\log 3}{\log q}} \sum_{k=1}^{\infty} \partial(p) f^k(p) (q^{-1}z)^{k\partial(p)}.$$
Hence, by Lemma 6.1.1,
$$\int_{\theta_0}^{\theta_0+\eta} \left| \frac{re^{i\theta} T_2'(re^{i\theta})}{T_2(re^{i\theta})} \right|^2 d\theta \le 2 \int_{-\eta}^{\eta} \left| \frac{q^{-1}re^{i\theta} Z'(q^{-1}re^{i\theta})}{Z(q^{-1}re^{i\theta})} \right|^2 d\theta,$$
and the argument in the proof of Lemma 6.1.3 yields
$$\int_{-\pi}^{\pi} \left| \frac{re^{i\theta} T_2'(re^{i\theta})}{T_2(re^{i\theta})} \right|^2 d\theta \ll \frac{1}{1-r}. \tag{1.14}$$

We now consider
$$\frac{T_1'(re^{i\theta})}{T_1(re^{i\theta})} = \sum_{\partial(p) \le \frac{\log 3}{\log q}} \frac{m'(re^{i\theta};p)}{1 + m(re^{i\theta};p)},$$

where

$$m(z;p) := \sum_{k=1}^{\infty} f(p^k)(q^{-1}z)^{k\partial(p)}$$

(by (1.5) and (1.6), $|m(z;p)| < 1$ for $|z| < 1$). We note that, for $|z| \le 1$,

$$|m'(z;p)| = \left|\sum_{k=1}^{\infty} k\partial(p) q^{-1} f(p^k)(q^{-1}z)^{k\partial(p)-1}\right| \ll 1.$$

Let

$$\frac{1}{1+m(z;p)} = 1 + \sum_{\ell=1}^{\infty}(\,-\,m(z;,p))^{\ell} = \sum_{a} g(a;p) z^{\partial(a)}.$$

Also, if $\partial(p) \ge \frac{\log 2}{\log q}$, let

$$1 + \sum_{\ell=1}^{\infty}\left(\sum_{k=1}^{\infty}(q^{-1}z)^{k\partial(p)}\right)^{\ell} = \sum_{a} h(a;p) z^{\partial(a)}.$$

Then $|g(a;p)| \le h(a;p)$ for all $a \in \mathcal{G}$, since $|f(p^k)| \le 1$. We note that

$$\begin{aligned}
\frac{1-(q^{-1}z)^{\partial(p)}}{1-2(q^{-1}z)^{\partial(p)}} &= \frac{1}{1-\sum\limits_{k=1}^{\infty}(q^{-1}z)^{k\partial(p)}} \\
&= 1 + \sum_{\ell=1}^{\infty}\left(\sum_{k=1}^{\infty}(q^{-1}z)^{k\partial(p)}\right)^{\ell}.
\end{aligned}$$

By Lemma 6.1.1, for $0 \le r < 1$,

$$\begin{aligned}
\int_{\theta_0}^{\theta_0+\eta} \frac{d\theta}{|1+m(re^{i\theta};p)|^2} &\le 2\int_{-\eta}^{\eta}\left|\frac{1-(q^{-1}re^{i\theta})^{\partial(p)}}{1-2(q^{-1}re^{i\theta})^{\partial(p)}}\right|^2 d\theta \\
&\ll \int_{-\eta}^{\eta}\frac{1}{\left|1-2(q^{-1}re^{i\theta})^{\partial(p)}\right|^2}d\theta \\
&= \int_{-\eta}^{\eta}\frac{d\theta}{1-4(q^{-1}r)^{\partial(p)}\cos(\partial(p)\theta)+4(q^{-1}r)^{2\partial(p)}} \\
&\le \left(\left[\frac{\eta\partial(p)}{\pi}\right]+1\right)\frac{2\pi}{\partial(p)}\,\frac{1}{1-4(q^{-1}r)^{2\partial(p)}} \\
&\ll \frac{1}{1-r^2},
\end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

since, by Poisson's integral formula,

$$\frac{1}{2\pi}\int_{-\pi}^{\pi}\frac{du}{1-4(q^{-1}r)^{\partial(p)}\cos u+4(q^{-1}r)^{2\partial(p)}}=\frac{1}{1-4(q^{-1}r)^{2\partial(p)}}\,.$$

If $\partial(p)<\frac{\log 2}{\log q}$, let

$$1+\sum_{\ell=1}^{\infty}\left(\sum_{k=k(p)}^{\infty}(q^{-1}z)^{k\partial(p)}\right)^{\ell}=\sum_{a}h(a;p)z^{\partial(a)}.$$

Then $|g(a;p)|\leq h(a;p)$ for all $a\in\mathcal{G}$ too, since $f(p^k)=0$ for all $1\leq k<k(p)$. Note that

$$\begin{aligned}\frac{1-(q^{-1}z)^{\partial(p)}}{1-(q^{-1}z)^{\partial(p)}-(q^{-1}z)^{k(p)\partial(p)}} &= \frac{1}{1-\sum\limits_{k=k(p)}^{\infty}(q^{-1}z)^{k\partial(p)}}\\ &= 1+\sum_{\ell=1}^{\infty}\left(\sum_{k=k(p)}^{\infty}(q^{-1}z)^{k\partial(p)}\right)^{\ell}.\end{aligned}$$

By Lemma 6.1.1 again, for $0\leq r<1$,

$$\begin{aligned}\int_{\theta_0}^{\theta_0+\eta}\frac{d\theta}{|1+m(re^{i\theta};p)|^2} &\leq 2\int_{-\eta}^{\eta}\left|\frac{1-(q^{-1}re^{i\theta})^{\partial(p)}}{1-(q^{-1}re^{i\theta})^{\partial(p)}-(q^{-1}re^{i\theta})^{k(p)\partial(p)}}\right|^2 d\theta\\ &\ll \int_{-\eta}^{\eta}\frac{d\theta}{\left|1-(q^{-1}re^{i\theta})^{\partial(p)}-(q^{-1}re^{i\theta})^{k(p)\partial(p)}\right|^2}\,.\end{aligned}$$

Note that $q^{\partial(p)}-1-q^{-\partial(p)(k(p)-1)}\geq 0$. If $q^{\partial(p)}-1-q^{-\partial(p)(k(p)-1)}>0$, then

$$\int_{\theta_0}^{\theta_0+\eta}\frac{d\theta}{|1+m(re^{i\theta};p)|^2}\ll_p 1,$$

since

$$\begin{aligned}&\left|1-(q^{-1}re^{i\theta})^{\partial(p)}-(q^{-1}re^{i\theta})^{k(p)\partial(p)}\right|\\ &\qquad\geq q^{-\partial(p)}\left[q^{\partial(p)}-1-q^{-\partial(p)(k(p)-1)}\right].\end{aligned}$$

If $q^{\partial(p)} - 1 - q^{-\partial(p)\left(k(p)-1\right)} = 0$, we have $1 = q^{-\partial(p)} + q^{-k(p)\partial(p)}$, and then

$$\begin{aligned}
&1 - (q^{-1}re^{i\theta})^{\partial(p)} - (q^{-1}re^{i\theta})^{k(p)\partial(p)} \\
&\quad = q^{-\partial(p)}\left(1 - (re^{i\theta})^{\partial(p)}\right) + q^{-k(p)\partial(p)}\left(1 - (re^{i\theta})^{k(p)\partial(p)}\right) \\
&\quad = -q^{-\partial(p)}\partial(p)\left[1 + k(p)q^{-\left(k(p)-1\right)\partial(p)}\right](\log r + i\theta) \\
&\qquad +O_p\left(|\log r + i\theta|^2\right),
\end{aligned}$$

for $k(p)\partial(p)|\log r + i\theta| < \frac{1}{2}$. Thus we can choose a positive number $\eta$ satisfying

$$\eta < \frac{1}{4k(p)\partial(p)},$$

so that, for $|\log r| \le \eta$, $|\theta| \le \eta$,

$$\left|1 - (q^{-1}re^{i\theta})^{\partial(p)} - (q^{-1}re^{i\theta})^{k(p)\partial(p)}\right|^2 \gg_\eta |\log r + i\theta|^2.$$

We note that there are only a finite number of $p$ with $\partial(p) < \frac{\log 2}{\log q}$. Hence we can fix $\eta > 0$ so that

$$\begin{aligned}
\int_{\theta_0}^{\theta_0+\eta} \frac{d\theta}{|1 + m(re^{i\theta};p)|^2} &\ll \int_{-\eta}^{\eta} \frac{d\theta}{|\log r + i\theta|^2} \\
&\ll \frac{1}{|\log r|} \le \frac{1}{1-r},
\end{aligned}$$

where the constant implied by $\ll$ is uniform. It now follows that

$$\begin{aligned}
&\int_{\theta_0}^{\theta_0+\eta} \left|\frac{re^{i\theta}T_1'(re^{i\theta})}{T_1(re^{i\theta})}\right|^2 d\theta \\
&\quad \ll \sum_{\partial(p)<\frac{\log 3}{\log q}} \int_{\theta_0}^{\theta_0+\eta} \left|\frac{m'(re^{i\theta};p)}{1 + m(re^{i\theta};p)}\right|^2 d\theta \\
&\quad \ll \frac{1}{1-r},
\end{aligned}$$

and then

$$\int_{-\pi}^{\pi} \left|\frac{re^{i\theta}T_1'(re^{i\theta})}{T_1(re^{i\theta})}\right|^2 d\theta \ll \frac{1}{1-r}. \tag{1.15}$$

Thus (1.10) follows from (1.13), (1.14), and (1.15). □

As the following lemma shows, either condition (1.8) or condition (1.9) can be replaced by the Chebyshev-type upper bound $\bar{\Lambda}(n) \ll q^n$. For brevity, an (additive) arithmetical semigroup $\mathcal{G}$ will be said to be a **Chebyshev** (additive) arithmetical semigroup if and only if $\bar{\Lambda}(n) \ll q^n$, or, equivalently, $P(n) \ll q^n/n$, holds in $\mathcal{G}$.

(6.1.5) LEMMA. *Assume that $\mathcal{G}$ is a Chebyshev arithmetical semigroup satisfying (1.7). Let $f$ be a completely multiplicative function such that $|f(a)| \leq 1$ for all $a \in \mathcal{G}$, or a multiplicative function satisfying the conditions of Lemma 6.1.2. Then (1.10) holds for $0 \leq r < 1$.*

PROOF. We first note that

$$\frac{q^{-1}zZ'(q^{-1}z)}{Z(q^{-1}z)} = \Lambda^{\#}(q^{-1}z) = \sum_{n=1}^{\infty} \bar{\Lambda}(n)(q^{-1}z)^n,$$

and hence

$$\int_{-\pi}^{\pi} \left| \frac{q^{-1}re^{i\theta}Z'(q^{-1}re^{i\theta})}{Z(q^{-1}re^{i\theta})} \right|^2 d\theta$$
$$= \sum_{n=1}^{\infty} (\bar{\Lambda}(n))^2 (q^{-1}r)^{2n} \ll \sum_{n=1}^{\infty} r^{2n} \ll \frac{1}{1-r}.$$

Then, in the case of a completely multiplicative function $f$, (1.10) follows from an argument similar to the one in the proof of Lemma 6.1.3. In the case of a multiplicative function $f$ satisfying the conditions of Lemma 6.1.2, (1.10) follows from an argument similar to the one in the proof of Lemma 6.1.4. □

### 6.1.2 Convolution of functions on (additive) arithmetical semigroups

In sub-section 3.1.1 earlier there was a brief discussion of the *additive* convolution $*_0$ of complex-valued functions of non-negative integers, which has parallels with the *multiplicative* (or *Dirichlet-type*) convolution $*_1$ of arithmetical functions on an arithmetical semigroup $\mathcal{G}$, treated in detail in Chapter 2 of [AB]. As noted earlier, the simpler single notation $*$ will be used in both cases, unless there is a need to avoid confusion between the two. For convenience in presenting the next sections, we now briefly recall or note a few basic properties of $* = *_1$ for the case when $\mathcal{G}$ is an *additive* arithmetical semigroup as before.

Firstly recall that the multiplicative convolution $*$, which is commutative and associative, and linear over complex scalar multiplication, is defined by

$$(f * g)(a) = \sum_{bc=a} f(b)g(c) \quad \text{for} \quad a \in \mathcal{G}.$$

Under $*$ the resulting algebra of all arithmetical functions on $\mathcal{G}$ has the identity element $\delta$, where $\delta(1) = 1$ and $\delta(a) = 0$ for $a \neq 1$ in $\mathcal{G}$. Also we have the following useful inequality

$$|f * g| \leq |f| * |g|, \tag{1.16}$$

which is easily verified. Another useful formula is

$$\sum_{\partial(a)=m} (f * g)(a) = \sum_{\partial(a)\leq m} F(m - \partial(a))g(a), \tag{1.17}$$

where $F(n) = \sum_{\partial(a)=n} f(a)$ is the *summatory* function of $f$. Actually, we have

$$\sum_{\partial(a)=m} (f * g)(a) \quad = \quad \sum_{\partial(a)=m} \sum_{bd=a} f(d)g(b)$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

$$\begin{aligned}
&= \sum_{\partial(b)+\partial(d)=m} f(d)g(b) \\
&= \sum_{\partial(b)\leq m} \left( \sum_{\partial(d)=m-\partial(b)} f(d) \right) g(b),
\end{aligned}$$

and (1.17) follows.

Next recall ([AB], Chap. 2, §2) that an arithmetical function $f$ is *invertible* relative to $*$, i.e. there exists a function $f^{-1}$ on $\mathcal{G}$ such that $f * f^{-1} = f^{-1} * f = \delta$, if and only if $f(1) \neq 0$, and then the inverse $f^{-1}$ is unique. Further ([AB], Chap. 2, §4), if $f$ and $g$ are both multiplicative on $\mathcal{G}$ then $f^{-1}$, $g^{-1}$ and $f * g$ are also multiplicative. (For $h = f * g$, this assertion may also be seen simply as follows: If $a$ and $b$ are coprime then every divisor $d$ of $ab$ can be uniquely written as $d = d_1 d_2$ with $d_1 \mid a$ and $d_2 \mid b$. Hence

$$\begin{aligned}
h(ab) &= \sum_{d|ab} f(d) g\left(\frac{ab}{d}\right) = \sum_{d_1|a,\, d_2|b} f(d_1 d_2) g\left(\frac{ab}{d_1 d_2}\right) \\
&= \left( \sum_{d_1|a} f(d_1) g\left(\frac{a}{d_1}\right) \right) \left( \sum_{d_2|b} f(d_2) g\left(\frac{b}{d_2}\right) \right) \\
&= h(a)h(b).)
\end{aligned}$$

The formal "differentiation" operator $L$ on the algebra of arithmetical functions of non-negative integers, discussed in sub-section 3.1.1 earlier, has an analogue for arithmetical functions $f$ on $\mathcal{G}$, defined by setting

$$Lf(a) = \partial(a) f(a) \text{ for } a \in \mathcal{G}.$$

Then $L$ is also a *derivation* (or formal "differentiation") operator, in view of the important property

$$L(f * g) = Lf * g + f * Lg.$$

(This is easily verified with the identity

$$\partial(a) \sum_{bd=a} f(d) g(b)$$

$$= \sum_{bd=a} (\partial(d)f(d))g(b) + \sum_{bd=a} f(d)(\partial(b)g(b)).)$$

Note that, if $F$ and $G$ are the summatory functions of $f$ and $g$, and $\hat{F}(y)$ and $\hat{G}(y)$ are generating functions $F$ and $G$ (or $f$ and $g$) respectively, then the generating function of the convolution $h = f * g$ is

$$\hat{H}(y) = \hat{F}(y)\hat{G}(y),$$

and the generating function of $Lf$ is

$$y\hat{F}'(y).$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

## 6.2 General Mean–Value Theorems

We shall formulate some general mean–value theorems in terms of slowly oscillating functions.

### 6.2.1 Slowly oscillating functions

Let $L(x)$ be a complex–valued function, defined and non–zero for all sufficiently large positive real numbers $x$. If

$$\lim_{x \to \infty} \frac{L(ux)}{L(x)} = 1 \tag{2.1}$$

holds for every fixed positive number $u$, then $L(x)$ is said to be *slowly oscillating.*

The most commonly used property of slowly oscillating functions is given in the following lemma, which in its present form is due to van Aardenne–Ehrenfest, de Bruijn and Korevaar [1].

(6.2.1) LEMMA. *Let $L$ be a measurable, slowly oscillating function. Then (2.1) holds uniformly for $u$ on any finite interval $a \leq u \leq b$ with $0 < a < b < \infty$.*

A short proof of this lemma is given in Elliott [1, Vol. I], Lemma 1.3.

### 6.2.2 The general mean–value theorems

We shall first prove the following general mean–value theorem, an analogue of *Halász's theorem* (cf. Halász [1], or Elliott [1], Vol. I) in classical proba-

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

bilistic number theory. As is well–known, in the classical theory, the values $f(2^k)$ of a multiplicative function $f$ on powers of 2 require special consideration. The same situation occurs in the theory of additive arithmetic semigroups when $\partial(p) \leq \frac{\log 2}{\log q}$. Thus we need extra constraints on the values $f(p^k)$ of $f$ on powers of such primes $p$ so that $f$ becomes tractable.

(6.2.2) THEOREM. (cf. Zhang [8]). *Suppose there exist a constant $c$, real constants $\alpha$ and $q > 1$, and a measurable, slowly oscillating function $L$ with $|L(x)| = 1$ such that*

$$F(m) = cq^{m(1+i\alpha)}L(m) + o(q^m) \tag{2.2}$$

*as $m \to \infty$. Then the asymptotic formula*

$$\hat{F}(y) = \frac{c}{1 - q^{1+i\alpha}y} L\left(\frac{1}{1 - q|y|}\right) + o\left(\frac{1}{1 - q|y|}\right) \tag{2.3}$$

*holds as $|y| \to q^{-1}-$.*

*Conversely, suppose that*

$$\sum_{n=1}^{\infty} \left|G(n)q^{-n} - A\right| < \infty, \tag{2.4}$$

*and either*

$$G(n)q^{-n} - A = O(n^{-1}) \tag{2.5}$$

*or*

$$\sum_{n=1}^{\infty} n\left(G(n)q^{-n} - A\right)^2 < \infty. \tag{2.6}$$

*Moreover, suppose $|f(a)| \leq 1$ for all $a \in \mathcal{G}$, and either*

*(i) $f$ is a completely multiplicative function on $\mathcal{G}$, or*

*(ii) $f$ is a multiplicative function such that, for each prime $p$ with $\partial(p) < \frac{\log 2}{\log q}$, there exists a positive integer $k(p)$ such that $q^{\partial(p)} - 1 - q^{\left(k(p)-1\right)\partial(p)} \geq 0$, and $f(p^k) = 0$ for all $1 \leq k < k(p)$.*

*Then (2.3) implies (2.2).*

The following proof is modelled after arguments in Elliott [1], in several aspects.

PROOF. Assume (2.2). Then

$$\begin{aligned}\hat{F}(y) &= \sum_{n=0}^{\infty}\left(cq^{n(1+i\alpha)}L(n)+o(q^n)\right)y^n\\ &= c\sum_{n=0}^{\infty}L(n)(q^{1+i\alpha}y)^n+o\left(\sum_{n=0}^{\infty}(q|y|)^n\right)\\ &= c\sum_{n=0}^{\infty}L(n)(q^{1+i\alpha}y)^n+o\left(\frac{1}{1-q|y|}\right)\end{aligned}$$

as $|y|\to q^{-1}-$. Let $M$ be a large positive constant, to be specified later, and let

$$M_1=M^{-1}(1-q|y|)^{-1},\quad M_2=M(1-q|y|)^{-1}.$$

By Lemma 6.2.1, we have

$$L(n)=L\left(\frac{1}{1-q|y|}\right)+o_M(1)$$

for $M_1\le n\le M_2$, and hence

$$\begin{aligned}&\sum_{M_1\le n\le M_2}L(n)(q^{1+i\alpha}y)^n\\ &\quad=L\left(\frac{1}{1-q|y|}\right)\sum_{M_1\le n\le M_2}(q^{1+i\alpha}y)^n+o_M\left(\frac{1}{1-q|y|}\right)\end{aligned}$$

as $|y|\to q^{-1}-$. It follows that

$$\begin{aligned}&\left|\hat{F}(y)-\frac{1}{1-q^{1+i\alpha}y}L\left(\frac{1}{1-q|y|}\right)\right|\\ &\quad=\left|c\sum_{n=0}^{\infty}L(n)(q^{1+i\alpha}y)^n+o\left(\frac{1}{1-q|y|}\right)\right.\end{aligned}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

$$-c\sum_{n=0}^{\infty} L\left(\frac{1}{1-q|y|}\right)\left(q^{1+i\alpha}y\right)^n\Bigg|$$

$$\le 2|c|\left\{\sum_{n<M_1}+\sum_{n>M_2}\right\}(q|y|)^n + o_M\left(\frac{1}{1-q|y|}\right).$$

We then have

$$\sum_{n<M_1}(q|y|)^n \le M_1 = M^{-1}(1-q|y|)^{-1},$$

and

$$\begin{aligned}\sum_{n>M_2}(q|y|)^n &= (q|y|)^{[M_2]+1}(1-q|y|)^{-1}\\ &\le e^{-\left(1-q|y|\right)M_2}(1-q|y|)^{-1}\\ &= e^{-M}(1-q|y|)^{-1}\end{aligned}$$

since $1-x<e^{-x}$. Therefore, we arrive at

$$\left|\hat{F}(y)-\frac{c}{1-q^{1+i\alpha}y}L\left(\frac{1}{1-q|y|}\right)\right|$$
$$\le 2|c|(M^{-1}+e^{-M})(1-q|y|)^{-1}+o_M\left((1-q|y|)^{-1}\right).$$

Given any $\varepsilon>0$, we can first choose $M$ sufficiently large so that the first term on the right–hand side is less than $\frac{\varepsilon}{2}(1-q|y|)^{-1}$. Then, for $|y|\to q^{-1}-$, the second term does not exceed $\frac{\varepsilon}{2}(1-q|y|)^{-1}$. Thus the right–hand side is less than $\varepsilon(1-q|y|)^{-1}$ for $|y|$ sufficiently close to $q^{-1}$, and (2.2) follows. This proves the first part of the theorem.

Conversely, we note that

$$\sum_{\partial(a)=n}|f(a)|\le G(n)\ll q^n$$

by (2.4), and hence the infinite series and infinite product in (0.1) converge absolutely for $|y|<q^{-1}$. We first assume (2.2) with $\alpha=0$, i.e.

$$\hat{F}(y)=\frac{c}{1-qy}L\left(\frac{1}{1-q|y|}\right)+o\left(\frac{1}{1-q|y|}\right)$$

for $|y| \to q^{-1}-$. To deduce (2.3) with $\alpha = 0$, we start with

$$\frac{1}{2\pi i} \int_{|y|=r} \frac{\hat{F}'(y)}{y^m}\, dy = mF(m),$$

where $0 < r < q^{-1}$. For simplicity of computation, let

$$T(z) := \hat{F}(q^{-1}z), \quad |z| < 1.$$

Then

$$\frac{q^m}{2\pi i} \int_{|z|=r} \frac{T'(z)}{z^m}\, dz = mF(m),$$

where $0 < r < 1$. To show (2.3) with $\alpha = 0$, it is sufficient to obtain

$$\frac{1}{2\pi i} \int_{|z|=r} \frac{T'(z)}{z^m}\, dz = cmL(m) + o(m). \tag{2.7}$$

To this end, we first have

$$T(z) = \hat{F}(q^{-1}z) = \frac{c}{1-z} L\left(\frac{1}{1-|z|}\right) + o\left(\frac{1}{1-|z|}\right) \tag{2.8}$$

as $|z| \to 1-$. Now, on the left-hand side of (2.7), we set $r = 1 - \frac{1}{m}$. Let $K$ be a large positive number and let $m$ be so large that $m \geq 2K^2$. We break the circle $z = re^{i\theta}$ into two arcs $A_0 : |\theta| \leq \frac{K}{m}$ and $A_1 : \frac{K}{m} \leq |\theta| \leq \pi$ and estimate the integral on the left–hand side of (2.7) on each arc separately. This will show that the integral on $A_0$ produces the main term on the right–hand side of (2.7), whereas the integral on $A_1$ produces an $o$–term.

(i) *Estimate of* $\int_{A_0}$. For $z \in A_0$, $z$ fixed for the moment, consider the circle $|w - z| = \frac{1}{2m}$. By (2.8) and Lemma 6.2.1, we have

$$\begin{aligned} T(w) &= \frac{c}{1-w} L\left(\frac{1}{1-|w|}\right) + o\left(\frac{1}{1-|w|}\right) \\ &= \frac{c}{1-w} L(m) + o(m), \end{aligned}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

since $1 - \frac{3}{2m} \le |w| \le 1 - \frac{1}{2m}$, and

$$L\left(\frac{1}{1-|w|}\right) = L(m) + o(1).$$

It follows, by Cauchy's inequality for derivatives of analytic functions, that

$$T'(z) = \frac{c}{(1-z)^2} L(m) + o(m^2).$$

Hence we have

$$\frac{1}{2\pi i}\int_{A_0} \frac{T'(z)}{z^m}\,dz = \frac{cL(m)}{2\pi i}\int_{A_0} \frac{dz}{(1-z)^2 z^m} + o(m^2)\frac{2K}{m}. \tag{2.9}$$

The integral on the right-hand side of (2.9) can be evaluated by using the residue theorem. Thus, let $r_m = \left|1 - \left(1 - \frac{1}{m}\right) e^{iK/m}\right|$ and let $C_1$ denote the path consisting of two line segments $z = \rho e^{\pm iK/m}$, $r \le \rho \le 1 + r_m$, and the circle arc: $z = (1+r_m)e^{i\theta}$, $|\theta| \le \frac{K}{m}$. We note that

$$\frac{K}{m} \gg r_m = \left[2\left(1 - \frac{1}{m}\right)\left(1 - \cos\frac{K}{m}\right) + \frac{1}{m^2}\right]^{1/2} \gg \frac{K}{m}.$$

Applying the residue theorem to the contour integral on $A_0 \cup C_1$, we obtain

$$\frac{1}{2\pi i}\int_{A_0} \frac{dz}{(1-z)^2 z^m} = m + \frac{1}{2\pi i}\int_{C_1} \frac{dz}{(1-z)^2 z^m}.$$

We have

$$\begin{aligned}\int_{C_1} \frac{dz}{(1-z)^2 z^m} &= -\int_r^{1+r_m} \frac{e^{iK/m}d\rho}{(1-\rho e^{iK/m})^2(\rho e^{iK/m})^m} \\ &+ \int_r^{1+r_m} \frac{e^{iK/m}d\rho}{(1-\rho e^{-iK/m})^2(\rho e^{-iK/m})^m} \\ &+ \int_{-K/m}^{K/m} \frac{(1+r_m)e^{i\theta}id\theta}{(1-(1+r_m)e^{i\theta})^2\left((1+r_m)e^{i\theta}\right)^m}.\end{aligned} \tag{2.10}$$

Note that $|1-\rho e^{\pm iK/m}| \geq \sin\frac{K}{m} \geq \frac{2K}{\pi m}$, and hence the first two integrals on the right-hand side of (2.10) are

$$\ll \left(\frac{K}{m}\right)^{-2} \int_r^\infty \frac{d\rho}{\rho^m} = \left(\frac{K}{m}\right)^{-2} \frac{\left(1-\frac{1}{m}\right)^{-m+1}}{m-1}.$$

Also, note that $\left|1-(1+r_m)e^{i\theta}\right| \geq r_m \gg \frac{K}{m}$, and hence the last integral on the right-hand side of (2.10) is

$$\ll \left(\frac{K}{m}\right)^{-1} \frac{2K}{m} \ll K^{-1}m.$$

It follows that

$$\frac{1}{2\pi i}\int_{A_0} \frac{dz}{(1-z)^2 z^m} = m + O(K^{-1}m). \tag{2.11}$$

(ii) *Estimate of* $\int_{A_1}$. By Lemma 6.1.2, $T(z) \neq 0$ for $|z|<1$. We have

$$\begin{aligned}\left|\int_{A_1} \frac{T'(z)}{z^m}\,dz\right| &\leq \left(\int_{A_1} \left|\frac{re^{i\theta}T'(re^{i\theta})}{T(re^{i\theta})}\right|^2 r^{-m}\,d\theta\right)^{1/2} \\ &\quad\times \left(\int_{A_1} \left|T(re^{i\theta})\right|^2 r^{-m}\,d\theta\right)^{1/2}.\end{aligned}$$

Then, by Lemma 6.1.3 in case of a function $f$ satisfying the condition (i) or by Lemma 6.1.4 in case of a function satisfying the condition (ii),

$$\int_{A_1} \left|\frac{re^{i\theta}T'(re^{i\theta})}{T(re^{i\theta})}\right|^2 r^{-m}\,d\theta \ll \frac{1}{1-r} = m.$$

Also we have

$$\int_{A_1} \left|T(re^{i\theta})\right|^2 r^{-m}\,d\theta \leq \max_{\frac{K}{m}\leq|\theta|\leq\pi} \left|T(re^{i\theta})\right|^{1/2} \int_{A_1} \left|T(re^{i\theta})\right|^{3/2} r^{-m}\,d\theta. \tag{2.12}$$

By (2.8),

$$\left|T(re^{i\theta})\right| \leq \left|\frac{c}{1-re^{i\theta}}\right| + o(m).$$

For $\frac{K}{m} \le |\theta| \le \pi$,

$$|1 - re^{i\theta}| \ge \left|1 - \left(1 - \frac{1}{m}\right) e^{iK/m}\right| = r_m \gg \frac{K}{m}$$

and hence

$$\max_{\frac{K}{m} \le |\theta| \le \pi} \left|T(re^{i\theta})\right|^{1/2} \le O\left(K^{-1/2} m^{1/2}\right) + o\left(m^{1/2}\right).$$

To estimate the integral on the right–hand side of (2.12), by Lemma 6.1.2, we have

$$\int_{A_1} \left|T(re^{i\theta})\right|^{3/2} r^{-m} d\theta \ll \int_{A_1} \left|T_2(re^{i\theta})\right|^{3/2} d\theta.$$

From the same lemma, we have, for $|z| < 1$,

$$(T_2(z))^{3/4} = \exp\left\{\frac{3}{4} \sum_{\partial(p) \ge \frac{\log 3}{\log q}} \sum_{k=1}^{\infty} \frac{1}{k} f^k(p) (q^{-1}z)^{k\partial(p)}\right\}.$$

Note that

$$\left(Z(q^{-1}z)\right)^{3/4} = \exp\left\{\frac{3}{4} \sum_{p} \sum_{k=1}^{\infty} \frac{1}{k} (q^{-1}z)^{k\partial(p)}\right\}.$$

By Lemma 6.1.1, we have

$$\begin{aligned} \int_{A_1} \left|T_2(re^{i\theta})\right|^{3/2} d\theta &\ll \int_{-\pi}^{\pi} \left|Z(q^{-1}re^{i\theta})\right|^{3/2} d\theta \\ &= \int_{-\pi}^{\pi} \left|\frac{A}{1 - re^{i\theta}} + R(q^{-1}re^{i\theta})\right|^{3/2} d\theta \\ &\ll 1 + \int_{-\pi}^{\pi} \left|\frac{1}{(1 - re^{i\theta})^{3/4}}\right|^2 d\theta. \end{aligned}$$

The last integral equals

$$\begin{aligned} &\int_{-\pi}^{\pi} \left(\sum_{k=0}^{\infty} \binom{k + \frac{3}{4} - 1}{k} r^k e^{ik\theta}\right) \left(\sum_{\ell=0}^{\infty} \binom{\ell + \frac{3}{4} - 1}{\ell} r^\ell e^{-i\ell\theta}\right) d\theta \\ = \;& 2\pi \sum_{k=0}^{\infty} \binom{k - \frac{1}{4}}{k}^2 r^{2k} \ll 1 + \sum_{k=1}^{\infty} k^{-1/2} r^{2k} \\ \ll \;& \frac{1}{(1 - r^2)^{1/2}} \ll m^{1/2}. \end{aligned}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

It follows that

$$\begin{aligned}\left|\int_{A_1} \frac{T'(z)}{z^m}\,dz\right| &\ll m^{1/2}\left\{\left[O\left(K^{-\frac{1}{2}}m^{\frac{1}{2}}\right)+o\left(m^{\frac{1}{2}}\right)\right]m^{\frac{1}{2}}\right\}^{1/2} \\ &\leq O\left(K^{-\frac{1}{4}}m\right)+o(m). \qquad (2.13)\end{aligned}$$

Combining (2.9), (2.11), and (2.13), we finally arrive at

$$\begin{aligned}&\frac{1}{2\pi i}\int_{|z|=r}\frac{T'(z)}{z^m}\,dz \\ &= \frac{cL(m)}{2\pi i}\int_{A_0}\frac{dz}{(1-z)^2z^m}+o(Km)+O\left(K^{-\frac{1}{4}}m\right) \\ &= cmL(m)+o(Km)+O\left(K^{-\frac{1}{4}}m\right).\end{aligned}$$

We note that the left–hand is independent of $K$. Hence, given $\varepsilon > 0$, the last term $O\left(K^{-\frac{1}{4}}m\right)$ on the right–hand side is less than $\frac{\varepsilon}{2}m$ for fixed $K$, sufficiently large. Then, for $m$ sufficiently large, $o(Km)$ does not exceed $\frac{\varepsilon}{2}m$. This proves (2.7), and hence (2.3) with $\alpha = 0$.

To finish the proof, now assume (2.3) with $\alpha \neq 0$. Then, for the function $f(a)q^{-i\partial(a)\alpha}$, its generating function satisfies

$$\begin{aligned}&\sum_a \left(f(a)q^{-i\partial(a)\alpha}\right)y^{\partial(a)} = \hat{F}(q^{i\alpha}y) \\ &= \frac{c}{1-qy}L\left(\frac{1}{1-q|y|}\right)+o\left(\frac{1}{1-q|y|}\right).\end{aligned}$$

The above argument yields

$$\sum_{\partial(a)=m} f(a)q^{-i\partial(a)\alpha} = cq^mL(m)+o(q^m).$$

Hence

$$\sum_{\partial(a)=m} f(a) = cq^{m(1+i\alpha)}L(m)+o(q^m). \qquad \square$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Theorem 6.2.2 has the following immediate consequence.

(6.2.3) COROLLARY. *Assume*

$$\sum_{n=1}^{\infty} \sup_{n\le m} \left|G(m)q^{-m} - A\right| < \infty, \tag{2.14}$$

*or, in particular, assume*

$$G(m) = Aq^m + O\left(q^m m^{-\gamma}\right) \tag{2.15}$$

*with* $\gamma > 1$. *Then (2.4) and (2.5) hold. Thus, for a function* $f$ *satisfying* $|f(a)| \le 1$ *for all* $a \in \mathcal{G}$ *and either condition (i) or (ii) of Theorem 6.2.2, (2.3) implies (2.2).*

As is seen in Section 6.1, either condition (2.5) (see (1.7)) or condition (2.6) (see (1.8)) can be replaced by a Chebyshev–type upper bound $\bar{\Lambda}(n) \ll q^n$.

(6.2.4) THEOREM. *Instead of either (2.5) or (2.6), assume that* $\mathcal{G}$ *is a Chebyshev additive arithmetical semigroup satisfying (2.4). Then, for a function* $f$ *satisfying* $|f(a)| \le 1$ *for all* $a \in \mathcal{G}$ *and either condition (i) or (ii) of Theorem 6.2.2, (2.3) implies (2.2).*

PROOF. The proof of Theorem 6.2.4 is the same as the one of Theorem 6.2.2, with the only difference that Lemma 6.1.5 is used now whereas Lemmas 6.1.3 and 6.1.4 were used in the latter. □

From Theorems 6.2.2 and 6.2.4, the theory of mean–value properties of multiplicative function may be developed in two parallel lines: one assumes condition (2.4) and either (2.5) or (2.6), and another assumes Chebyshev semigroups satisfying (2.4). For simplicity, in the further discussion, we *consider only* Chebyshev semigroups satisfying (2.4), and omit the parallel results for semigroups satisfying (2.4) and either (2.5) or (2.6).

## 6.3 An Analogue of the Halász–Wirsing Theorem

The following theorem is an analogue of the *Halász–Wirsing theorem* in classical probabilistic number theory (cf. Halász [1], Wirsing [2], and Elliott [1]). There are no extra constraints on values of $f(p^k)$ on powers of primes $p$ with $\partial(p) < \frac{\log 2}{\log q}$ in this theorem.

(6.3.1) THEOREM. (cf. Zhang [8]). *Suppose either (i) that $\mathcal{G}$ is a Chebyshev additive arithmetical semigroup satisfying (2.4), or (ii) that (2.14) holds. Let $f$ be a multiplicative function with $|f(a)| \leq 1$ for all $a \in \mathcal{G}$. If there exists a real number $\alpha$ such that*

$$\sum_p q^{-\partial(p)} \left(1 - Re\left(f(p)q^{-i\theta\partial(p)}\right)\right) \tag{3.1}$$

*converges for $\theta = \alpha$, then*

$$\begin{aligned} F(m) &= Aq^{m(1+i\alpha)} \prod_{\partial(p)\leq m} \left(1 - q^{-\partial(p)}\right) \left(1 + \sum_{k=1}^{\infty} q^{-k\partial(p)(1+i\alpha)} f(p^k)\right) \\ &\quad + o(q^m) \end{aligned} \tag{3.2}$$

*as $m \to \infty$. On the other hand, if there exists no such $\alpha$, then*

$$F(m) = o(q^m).$$

*Remark.* Condition (ii) of this theorem implies condition (i), and is actually a particular case of the latter. However, we emphasize condition (ii) in the theorem, for its convenience of applications. In particular, if we assume (2.15) with $\gamma > 1$, then (2.14) holds.

To prove Theorem 6.3.1, we need two more lemmas.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

(6.3.2) LEMMA. *Assume (2.4), and $|f(p)| \leq 1$ for all $p \in \mathcal{P}$. If*

$$\sum_p q^{-\partial(p)}(1 - Ref(p)) < \infty, \tag{3.3}$$

*then we have, for each fixed $M > 0$, uniformly for $y = re^{i\theta}$ with $|\theta| \leq M(q^{-1} - \eta)$ and $\frac{1}{2}(q^{-1} - \eta) \leq q^{-1} - r \leq q^{-1} - \eta$,*

$$\sum_p \left|\eta^{\partial(p)} - y^{\partial(p)}\right| |1 - f(p)| = o(1) \tag{3.4}$$

*as $\eta \longrightarrow q^{-1}-$.*

PROOF. It suffices to show that

$$S_1 := \sum_p \left|\eta^{\partial(p)} - y^{\partial(p)}\right| (1 - Ref(p)) = o(1), \tag{3.5}$$

and

$$S_2 := \sum_p \left|\eta^{\partial(p)} - y^{\partial(p)}\right| |Im\, f(p)| = o(1). \tag{3.6}$$

Firstly, by (3.3),

$$\begin{aligned} S_1 &\leq 2 \sum_{\partial(p) \leq M_1} \left|\eta^{\partial(p)} - y^{\partial(p)}\right| + 2 \sum_{\partial(p) > M_1} q^{-\partial(p)}(1 - Ref(p)) \\ &\leq 2 \sum_{\partial(p) \leq M_1} \left|\eta^{\partial(p)} - y^{\partial(p)}\right| + \varepsilon, \end{aligned}$$

for $M_1$ sufficiently large. Fixing $M_1$, we have

$$\limsup_{n \rightarrow q^{-1}-} S_1 \leq \varepsilon,$$

since $y \rightarrow q^{-1}$ as $n \rightarrow q^{-1}-$. Then (3.5) follows.

Next, to show (3.6), first note that

$$\sum_p \left|\eta^{\partial(p)} - y^{\partial(p)}\right| \ll_M 1.$$

Actually,

$$\begin{aligned}\left|\left(\frac{\eta}{r}\right)^{\partial(p)} - e^{i\theta\partial(p)}\right| &\le \left|1 - \left(\frac{\eta}{r}\right)^{\partial(p)}\right| + \left|1 - e^{i\theta\partial(p)}\right| \\ &\le \partial(p)\left(-\log\frac{\eta}{r} + |\theta|\right),\end{aligned}$$

since $r \ge \eta$. Hence

$$\begin{aligned}\sum_p \left|\eta^{\partial(p)} - y^{\partial(p)}\right| &\le \sum_p \partial(p) r^{\partial(p)}\left(\log\frac{r}{\eta} + |\theta|\right) \\ &\le \sum_p \partial(p) r^{\partial(p)}\left(2q(q^{-1}-r) + 2M(q^{-1}-r)\right) \\ &\ll (q^{-1}-r)\sum_p \partial(p) r^{\partial(p)} \\ &\ll -(q^{-1}-r)\frac{rZ'(r)}{Z(r)} \ll 1,\end{aligned}$$

since

$$\log\frac{r}{\eta} \le \frac{r-\eta}{\eta} \le 2q(q^{-1}-r).$$

Then

$$\begin{aligned}S_2 &\le \varepsilon \sum_{|Im\, f(p)|<\varepsilon} \left|\eta^{\partial(p)} - y^{\partial(p)}\right| + \sum_{|Im\, f(p)|\ge\varepsilon} \left|\eta^{\partial(p)} - y^{\partial(p)}\right| \\ &\le M_2\varepsilon + \frac{1}{1-\sqrt{1-\varepsilon^2}}\sum_p \left|\eta^{\partial(p)} - y^{\partial(p)}\right|(1 - Re\, f(p)),\end{aligned}$$

since $1 - Re\, f(p) \ge 1 - \sqrt{1-\varepsilon^2}$ for $|Im\, f(p)| < \varepsilon$ ($|f(p)| \le 1$!). It follows from (3.5) that

$$\limsup_{\eta\to q^{-1}-} S_2 \le M_2\varepsilon,$$

and then (3.6) follows. □

(6.3.2) LEMMA. *Suppose that (2.4) holds. Let $f$ be a multiplicative function with $|f(a)| \le 1$ for all $a \in \mathcal{G}$. If (3.3) holds, then, for each fixed $M > 0$, uniformly for $y = re^{i\theta}$ with $M(1-q|y|) \le |\theta| \le \pi$,*

$$|\hat{F}(y)| \ll M^{-\frac{1}{2}}(1-q|y|)^{-1}.$$

PROOF. For $|y| < q^{-1}$,

$$\hat{F}(y) = \prod_p \left(1 + \sum_{k=1}^{\infty} f(p^k) y^{k\partial(p)}\right)$$

and so

$$\frac{\hat{F}(y)}{Z(|y|)} = \Pi_1(y) \prod_{\partial(p) < \frac{\log 3}{\log q}} \left(1 - |y|^{\partial(p)}\right) \left(1 + \sum_{k=1}^{\infty} f(p^k) y^{k\partial(p)}\right),$$

where

$$\begin{aligned} \Pi_1(y) : &= \prod_{\partial(p) \geq \frac{\log 3}{\log q}} \left(1 - |y|^{\partial(p)}\right) \left(1 + \sum_{k=1}^{\infty} f(p^k) y^{k\partial(p)}\right) \\ &= \exp\left\{ \sum_{\partial(p) \geq \frac{\log 3}{\log q}} \left(-|y|^{\partial(p)} + f(p) y^{\partial(p)}\right) + R_1(y) \right\}, \end{aligned}$$

with

$$\begin{aligned} R_1(y) &= \sum_{\partial(p) \geq \frac{\log 3}{\log q}} \left\{ -\sum_{k=2}^{\infty} \frac{|y|^{k\partial(p)}}{k} + \sum_{k=2}^{\infty} f(p^k) y^{k\partial(p)} \right. \\ &\qquad \left. + \sum_{\ell=2}^{\infty} \frac{(-1)^{\ell-1}}{\ell} \left( \sum_{k=1}^{\infty} f(p^k) y^{k\partial(p)} \right)^{\ell} \right\}. \end{aligned}$$

It is easy to see that, for $|y| < q^{-1}$,

$$\begin{aligned} |R_1(y)| &\ll \sum_{\partial(p) \geq \frac{\log 3}{\log q}} \left\{ \frac{q^{-2\partial(p)}}{1 - q^{-\partial(p)}} + \sum_{\ell=2}^{\infty} \frac{1}{\ell} \left( \frac{q^{-\partial(p)}}{1 - q^{-\partial(p)}} \right)^{\ell} \right\} \\ &\ll \sum_{\partial(p) \geq \frac{\log 3}{\log q}} q^{-2\partial(p)} \ll Z(q^{-2}) \ll 1. \end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Thus

$$\begin{aligned}\left|\frac{\hat{F}(y)}{Z(|y|)}\right| &\ll |\Pi_1(y)| \\ &\ll \exp\left\{-\sum_{\partial(p)\geq\frac{\log 3}{\log q}} |y|^{\partial(p)}\left(1-Re(f(p)e^{i\theta\partial(p)})\right)\right\}. \qquad (3.7)\end{aligned}$$

Note that

$$\frac{Z(|y|)}{Z(\bar{y})} = \Pi_2(y)\prod_{\partial(p)<\frac{\log 3}{\log q}}\left(1-|y|^{\partial(p)}\right)^{-1}\left(1-\bar{y}^{\partial(p)}\right),$$

where $\bar{y}$ is the complex conjugate of $y$ and

$$\begin{aligned}\Pi_2(y) :&= \prod_{\partial(p)\geq\frac{\log 3}{\log q}}\left(1-|y|^{\partial(p)}\right)^{-1}\left(1-\bar{y}^{\partial(p)}\right) \\ &= \exp\left\{\sum_{\partial(p)\geq\frac{\log 3}{\log q}}\left(|y|^{\partial(p)}-\bar{y}^{\partial(p)}\right)+R_2(y)\right\},\end{aligned}$$

with $|R_2(y)| \ll 1$ for $|y| \leq q^{-1}$. Thus

$$\begin{aligned}\left|\frac{Z(|y|)}{Z(\bar{y})}\right| &\ll |\Pi_2(y)| \\ &\ll \exp\left\{\sum_{\partial(p)\geq\frac{\log 3}{\log q}} |y|^{\partial(p)}\left(1-Re\, e^{-i\theta\partial(p)}\right)\right\}. \qquad (3.8)\end{aligned}$$

It follows from (3.7), (3.8), and (3.1) that

$$\begin{aligned}\frac{|\hat{F}(y)|^2}{Z(|y|)|Z(\bar{y})|} \ll \exp\Bigg\{&-2\sum_{\partial(p)\geq\frac{\log 3}{\log q}} |y|^{\partial(p)}\left(1-Re(f(p)e^{i\theta\partial(p)})\right) \\ &+\sum_{\partial(p)\geq\frac{\log 3}{\log q}} |y|^{\partial(p)}\left(1-Re\, e^{-i\theta\partial(p)}\right)\Bigg\}\end{aligned}$$

$$\begin{aligned} &\ll \exp\left\{2 \sum_{\partial(p)\geq \frac{\log 3}{\log q}} |y|^{\partial(p)} \left(1 - Re\, f(p)\right)\right\} \\ &\ll 1, \end{aligned}$$

since

$$\begin{aligned} 2\left(1 - Re\, e^{-i\theta\partial(p)}\right) &= \left|1 - e^{-i\theta\partial(p)}\right|^2 \\ &\leq 2|1 - f(p)|^2 + 2\left|f(p) - e^{-i\theta\partial(p)}\right|^2 \\ &\leq 4\left(1 - Re\, f(p)\right) + 4\left(1 - Re(f(p)e^{-i\theta\partial(p)})\right). \end{aligned}$$

Hence

$$\begin{aligned} |\hat{F}(y)| &\ll (Z(|y|)|Z(\bar{y})|)^{1/2} \ll \left(\frac{1}{(1-q|y|)|1-q\bar{y}|}\right)^{1/2} \\ &\ll \left(\frac{1}{(1-q|y|)M(1-q|y|)}\right)^{1/2} = M^{-1/2}(1-q|y|)^{-1}, \end{aligned}$$

since, for $M(1 - q|y|) \leq |\theta| \leq \pi$,

$$\begin{aligned} |1 - q\bar{y}| &\geq \left|1 - q|y|e^{iM(1-q|y|)}\right| \\ &= \left[(1-q|y|)^2 + 2q|y|\left(1 - \cos\left(M(1-q|y|)\right)\right)\right]^{1/2} \\ &\gg M(1-q|y|). \qquad \square \end{aligned}$$

*Proof of Theorem 6.3.1.* We note, from Theorem 3.2.1 of Chapter 3, that an additive arithmetical semigroup satisfying the condition (2.14) is a Chebyshev semigroup. It is sufficient to prove the theorem under the assumption (i). We shall write $f$ as the convolution of special functions $g$ and $h$ as follows:

Define multiplicative functions $g$ and $h$ by setting

$$g(p^k) = \begin{cases} f(p^k), & \text{if } \partial(p) < \frac{\log 2}{\log q}, \\ 0, & \text{if } \partial(p) \geq \frac{\log 2}{\log q}, \end{cases}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

and

$$h(p^k) = \begin{cases} 0, & \text{if } \partial(p) < \frac{\log 2}{\log q}, \\ f(p^k), & \text{if } \partial(p) \geq \frac{\log 2}{\log q}, \end{cases}$$

respectively. Then $g * h$ is multiplicative too, and $g(1) = 1 = h(1)$. It is easily verified, from the definition of $g$ and $h$, that $f(p^k) = (g * h)(p^k)$ for all powers of primes $p$. Hence $f = g * h$. Then

$$\sum_p q^{-\partial(p)} \left(1 - Re(h(p)q^{-i\theta\partial(p)})\right) \tag{3.9}$$

converges or diverges according as (3.1) converges or diverges.

First assume that (3.1), and hence (3.9), diverges for all real $\theta$. From the proof of Lemma 3.2 with $h$ in place of $f$, we have, for $|y| < q^{-1}$,

$$\frac{|\hat{H}(y)|}{Z(|y|)} \ll \exp\left\{- \sum_{\partial(p) \geq \frac{\log 3}{\log q}} |y|^{\partial(p)} \left(1 - Re(h(p)e^{i\theta\partial(p)})\right)\right\}.$$

From this fact,

$$\frac{|\hat{H}(y)|}{Z(|y|)} \to 0$$

as $y = re^{i\theta} \to q^{-1}e^{i\theta}$, with $r \to q^{-1}-$ for $0 \leq \theta \leq 2\pi$. By Dini's theorem (cf. Courant and Hilbert [1], Chapter 2, §2), this convergence is uniform for $0 \leq \theta \leq 2\pi$. Hence

$$\frac{|\hat{H}(y)|}{Z(|y|)} = o(1)$$

as $|y| \to q^{-1}-$. Also, note that

$$Z(|y|) \ll (1 - q|y|)^{-1}.$$

Thus

$$\hat{H}(y) = o\left((1 - q|y|)^{-1}\right).$$

Then, by Theorem 6.2.2,

$$H(m) = \sum_{\partial(a)=m} h(a) = o(q^m).$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Therefore we have, by (1.17),

$$\begin{aligned} F(m) &= \sum_{\partial(a)=m} (g * h)(a) = \sum_{\partial(a)\leq m} H(m-\partial(a))g(a) \\ &= \sum_{\partial(a)=m} g(a) + \sum_{\partial(a)<m} o(q^{m-\partial(a)})g(a). \end{aligned} \tag{3.10}$$

Note that

$$K := \sum_{a} q^{-\partial(a)}|g(a)| = \prod_{\partial(p)<\frac{\log 2}{\log q}} \left(1 + \sum_{k=1}^{\infty} q^{-k\partial(p)}|f(p^k)|\right) < \infty.$$

Therefore, given $0 < \varepsilon < \infty$

$$\sum_{\partial(a)\geq M_1} q^{-\partial(a)}|g(a)| < \varepsilon$$

for $M_1$ sufficiently large. Hence

$$\left|\sum_{\partial(a)=m} g(a)\right| \leq q^m \sum_{\partial(a)\geq m} q^{-\partial(a)}|g(a)| < \varepsilon q^m \tag{3.11}$$

for $m > M_1$. To estimate the second term on the right-hand side of (3.10) we note that, for $m - \partial(a) > M_2$ with $M_2$ sufficiently large,

$$\left|o\left(q^{m-\partial(a)}\right) g(a)\right| < \varepsilon q^{m-\partial(a)}|g(a)|,$$

and hence

$$\left|\sum_{\partial(a)<m-M_2} o\left(q^{m-\partial(a)}\right) g(a)\right| < \varepsilon K q^m.$$

Also, there exists a constant $B > 0$ such that

$$o\left(q^{m-\partial(a)}\right) \leq B q^{m-\partial(a)}$$

for $\partial(a) < m$, and hence

$$\left|\sum_{M_1\leq\partial(a)<m} o\left(q^{m-\partial(a)}\right) g(a)\right| \leq \varepsilon B q^m.$$

It follows that

$$\begin{aligned}
&\left| \sum_{\partial(a)<m} o\left(q^{m-\partial(a)}\right) g(a) \right| \\
&= \left| \left( \sum_{\partial(a)<m-M_2} + \sum_{m-M_2\leq\partial(a)<m} \right) o\left(q^{m-\partial(a)}\right) g(a) \right| \\
&\leq \varepsilon(K+B)q^m \qquad (3.12)
\end{aligned}$$

for $m > M_1 + M_2$. Then $F(m) = o(q^m)$ follows from (3.10), (3.11), and (3.12).

Assume now that (3.1), and hence (3.9), converges for $\theta = 0$. Then, as in the proof of Lemma 6.3.2,

$$\frac{\hat{H}(y)}{Z(y)} = H_1(y) \exp\left\{ - \sum_{\partial(p)\geq\frac{\log 3}{\log q}} y^{\partial(p)}(1-f(p)) \right\}, \qquad (3.13)$$

where

$$\begin{aligned}
H_1(y) : \;=\; & \prod_{\frac{\log 2}{\log q}\leq\partial(p)<\frac{\log 3}{\log q}} \left(1+\sum_{k=1}^{\infty} f(p^k)y^{k\partial(p)}\right) \prod_{\partial(p)<\frac{\log 3}{\log q}} (1-y^{\partial(p)}) \\
& \times \prod_{\partial(p)\geq\frac{\log 3}{\log q}} \left(1+\sum_{k=2}^{\infty} \left(f(p^k)-f(p^{k-1})f(p)\right) y^{k\partial(p)}\right) \\
& \times \exp\left\{ - \sum_{\partial(p)\geq\frac{\log 3}{\log q}} \sum_{k=2}^{\infty} \frac{1}{k} \left(1-f^k(p)\right) y^{k\partial(p)} \right\}
\end{aligned}$$

is holomorphic for $|y| < q^{-\frac{1}{2}}$. Set

$$c_1 = H_1(q^{-1}) \exp\left\{ - \sum_{\partial(p)\geq\frac{\log 3}{\log q}} q^{-\partial(p)}\left(1 - Re\, f(p)\right) \right\}$$

and

$$L\left(\frac{1}{1-q|y|}\right) = \exp\left\{ i \sum_{\partial(p)\geq\frac{\log 3}{\log q}} |y|^{\partial(p)} Im\, f(p) \right\}.$$

Clearly, $|L| = 1$. Let $u = (1 - q|y|)^{-1}$. To show that $L(u)$ is a slowly oscillating function of $u$, it suffices to note that, for $\frac{1}{2}u \leq v \leq u$, by Lemma 6.3.1 with $\eta = q^{-1}(1 - v^{-1})$,

$$\begin{aligned} \frac{L(v)}{L(u)} &= \exp\left\{ i \sum_{\partial(p) \geq \frac{\log 3}{\log q}} \left(\eta^{\partial(p)} - |y|^{\partial(p)}\right) Im\, f(p) \right\} \\ &= \exp\{o(1)\} \end{aligned}$$

as $u \to \infty$. Then, by the same lemma,

$$\begin{aligned} \frac{\hat{H}(y)}{L\left(\frac{1}{1-q|y|}\right) Z(y)} &= H_1(y) \exp\left\{ - \sum_{\partial(p) \geq \frac{\log 3}{\log q}} \left(y^{\partial(p)} - |y|^{\partial(p)}\right)(1 - f(p)) \right. \\ &\qquad \left. - \sum_{\partial(p) \geq \frac{\log 3}{\log q}} |y|^{\partial(p)}(1 - Re\, f(p)) \right\} \\ &= (c_1 + o_M(1)) \exp\{o_M(1) + o(1)\}, \end{aligned}$$

as $|y| \to q^{-1}-$ uniformly for $|\theta| \leq M(1 - q|y|)$. Hence

$$\hat{H}(y) = c_1 Z(y) L\left(\frac{1}{1 - q|y|}\right) + o_M\left((1 - q|y|)^{-1}\right).$$

Also, for $M(1 - q|y|) \leq |\theta|$, by Lemma 6.3.2,

$$\hat{H}(y) - c_1 Z(y) L\left(\frac{1}{1 - q|y|}\right) \ll M^{-\frac{1}{2}}(1 - q|y|)^{-1}.$$

Thus we have

$$\begin{aligned} \hat{H}(y) &= c_1 Z(y) L\left(\frac{1}{1 - q|y|}\right) + o\left((1 - q|y|)^{-1}\right) \\ &= \frac{c_1 A}{1 - qy} L\left(\frac{1}{1 - q|y|}\right) + o\left((1 - q|y|)^{-1}\right) \end{aligned}$$

as $|y| \to q^{-1}-$. By Theorem 6.2.4,

$$H(m) = c_1 A q^m L(m) + o(q^m).$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Then we obtain

$$F(m)=\sum_{\partial(a)\le m}H(m-\partial(a))g(a)=\sum_{\partial(a)=m}g(a)+S_1+S_2,$$

say, where

$$S_1:=c_1A\sum_{\partial(a)<m}q^{m-\partial(a)}L(m-\partial(a))g(a),$$

and

$$S_2:=\sum_{\partial(a)<m}o(q^{m-\partial(a)})g(a)=o(q^m),$$

as is shown above. Write

$$\begin{aligned}S_1 &= c_1A\Bigg\{q^mL(m)\sum_{\partial(a)\le M_1}q^{-\partial(a)}g(a)\\ &\quad+\sum_{\partial(a)\le M_1}q^{m-\partial(a)}\left(L(m-\partial(a))-L(m)\right)g(a)\Bigg\}\\ &\quad+c_1A\sum_{M_1<\partial(a)<m}q^{m-\partial(a)}L(m-\partial(a))g(a).\end{aligned}$$

Let $c=c_1\sum_a q^{-\partial(a)}g(a)$. Then

$$|S_1-cAq^mL(m)|\le\varepsilon|c_1|A(K+1)q^m,$$

for $m\ge M_1+M_3$ with $M_3$ sufficiently large, since

$$|L(m-\partial(a))-L(m)|=\left|\frac{L(m-\partial(a))}{L(m)}-1\right|<\varepsilon$$

uniformly for $\partial(a)\le M_1$. Hence we arrive at

$$F(m)=cAq^mL(m)+o(q^m).$$

It remains to show

$$cL(m)=\prod_{\partial(p)\le m}(1-q^{-\partial(p)})\left(1+\sum_{k=1}^{\infty}q^{-k\partial(p)}f(p^k)\right)+o(1). \tag{3.14}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Actually, let $1 - qr = m^{-1}$. Then $q^{-1} = r + (qm)^{-1}$, and thus

$$\begin{aligned} cL(m) &= (H_1(r) + o(1)) \left( \exp\left\{ - \sum_{\partial(p) \geq \frac{\log 3}{\log q}} r^{\partial(p)}(1 - Re\, f(p)) \right\} + o(1) \right) \\ &\quad \times \exp\left\{ i \sum_{\partial(p) \geq \frac{\log 3}{\log q}} r^{\partial(p)} Im\, f(p) \right\} \\ &\quad \times \prod_{\partial(p) < \frac{\log 2}{\log q}} \left( 1 + \sum_{k=1}^{\infty} q^{-k\partial(p)} f(p^k) \right) \\ &= H_1(r) \exp\left\{ - \sum_{\partial(p) \geq \frac{\log 3}{\log q}} r^{\partial(p)}(1 - f(p)) \right\} \\ &\quad \times \prod_{\partial(p) < \frac{\log 2}{\log q}} \left( 1 + \sum_{k=1}^{\infty} r^{k\partial(p)} f(p^k) \right) + o(1), \end{aligned}$$

since

$$\sum_{\partial(p) \geq \frac{\log 3}{\log q}} q^{-\partial(p)}(1 - Re\, f(p)) = \sum_{\partial(p) \geq \frac{\log 3}{\log q}} r^{\partial(p)}(1 - Re\, f(p)) + o(1)$$

as $r \to q^{-1}-$, by the convergence of (3.1) with $\theta = 0$, and $0 \leq r^{\partial(p)}(1 - Re\, f(p)) \leq q^{-\partial(p)}(1 - Re\, f(p))$. Then by (3.13),

$$cL(m) = \frac{\hat{F}(r)}{Z(r)} + o(1) \tag{3.15}$$

since

$$\hat{H}(r) \prod_{\partial(p) < \frac{\log 2}{\log q}} \left( 1 + \sum_{k=1}^{\infty} r^{k\partial(p)} f(p^k) \right) = \hat{F}(r).$$

We have

$$\frac{\hat{F}(r)}{Z(r)} = \prod_{p} (1 - r^{\partial(p)}) \left( 1 + \sum_{k=1}^{\infty} f(p^k) r^{k\partial(p)} \right). \tag{3.16}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Note that

$$\begin{aligned}\sum_{\partial(p)>m} r^{\partial(p)} &= \sum_{n=m+1}^{\infty} P(n)r^n \ll \sum_{n=m+1}^{\infty} n^{-1}q^n r^n \\ &\le \frac{1}{m}\sum_{n=m+1}^{\infty}\left(1-\frac{1}{m}\right)^n = \frac{1}{m}\,\frac{\left(1-\frac{1}{m}\right)^{m+1}}{\frac{1}{m}} \\ &\ll 1.\end{aligned}$$

Hence, by the Cauchy–Schwarz inequality,

$$\begin{aligned}\sum_{\partial(p)>m} r^{\partial(p)}|1-f(p)| &\le \left\{\sum_{\partial(p)>m} r^{\partial(p)}\right\}^{1/2}\left\{2\sum_{\partial(p)>m} r^{\partial(p)}(1-Re\, f(p))\right\}^{1/2} \\ &= o(1).\end{aligned}$$

Thus

$$\begin{aligned}&\prod_{\partial(p)>m}(1-r^{\partial(p)})\left(1+\sum_{k=1}^{\infty} f(p^k)r^{k\partial(p)}\right) \\ &\quad = \exp\left\{-\sum_{\partial(p)>m} r^{\partial(p)}(1-f(p))+o(1)\right\} \\ &\quad = \exp\{o(1)\}. \qquad (3.17)\end{aligned}$$

Also,

$$\begin{aligned}\sum_{\partial(p)\le m}(q^{-\partial(p)}-r^{\partial(p)}) &= \sum_{n\le m} P(n)(q^{-n}-r^n) \\ &\ll \sum_{n\le m}\frac{q^n}{n}(q^{-n}-r^n) = \sum_{n\le m}\frac{1}{n}(1-(qr)^n) \\ &= \sum_{n\le m}\frac{1}{n}\left(1-\left(1-\frac{1}{m}\right)^n\right) \\ &\le \sum_{n\le m}\frac{1}{n}\left(1-\left(1-\frac{n}{m}\right)\right) \\ &= 1\end{aligned}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

since, by Bernoulli's inequality,

$$\left(1-\frac{1}{m}\right)^n \geq 1-\frac{n}{m}\,.$$

Hence, by the Cauchy–Schwarz inequality again,

$$\begin{aligned}
&\sum_{\partial(p)\leq m} (q^{-\partial(p)} - r^{\partial(p)})|1-f(p)| \\
&\quad \leq \left\{\sum_{\partial(p)\leq m} (q^{-\partial(p)} - r^{\partial(p)})\right\}^{1/2} \\
&\qquad \times \left\{2\sum_{\partial(p)\leq m} (q^{-\partial(p)} - r^{\partial(p)})(1-Re\, f(p))\right\}^{1/2} \\
&\quad = o(1), \qquad\qquad (3.18)
\end{aligned}$$

since

$$\sum_{\partial(p)\leq m} (q^{-\partial(p)} - r^{\partial(p)})(1-Re\, f(p)) = o(1)$$

as $m \to \infty$, by the convergence of (3.1) with $\theta = 0$. Thus

$$\begin{aligned}
&\prod_{\partial(p)\leq m} (1-r^{\partial(p)})\left(1+\sum_{k=1}^{\infty} r^{k\partial(p)} f(p^k)\right) \\
&\quad = \prod_{\partial(p)<\frac{\log 3}{\log q}} (1-r^{\partial(p)})\left(1+\sum_{k=1}^{\infty} r^{k\partial(p)} f(p^k)\right) \\
&\qquad \times \prod_{\frac{\log 3}{\log q}\leq\partial(p)\leq m} (1-q^{-\partial(p)})\left(1+\sum_{k=1}^{\infty} q^{-k\partial(p)} f(p^k)\right) \\
&\qquad \times \exp\{R(r)\},
\end{aligned}$$

where

$$\begin{aligned}
R(r) \;=\; \sum_{\frac{\log 3}{\log q}\leq\partial(p)\leq m} &\Big[\log(1-r^{\partial(p)}) + \log(1-q^{-\partial(p)})^{-1} \\
&+\log(1-r^{\partial(p)}f(p))^{-1} + \log(1-q^{-\partial(p)}f(p))
\end{aligned}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

$$
\begin{aligned}
&\qquad + \log\left(1+\sum_{k=2}^{\infty} r^{k\partial(p)}\left(f(p^k)-f(p^{k-1})f(p)\right)\right) \\
&\qquad + \log\left(1+\sum_{k=2}^{\infty} q^{-k\partial(p)}\left(f(p^k)-f(p^{k-1})f(p)\right)\right)^{-1}\Bigg] \\
= &\sum_{\frac{\log 3}{\log q}\leq\partial(p)\leq m}\Bigg[(q^{-\partial(p)}-r^{\partial(p)})(1-f(p)) \\
&\qquad + \sum_{\ell=2}^{\infty}\frac{1}{\ell}\left(q^{-\ell\partial(p)}-r^{\ell\partial(p)}\right)\left(1-(f(p))^{\ell}\right) \\
&\qquad + \sum_{\ell=1}^{\infty}\frac{1}{\ell}\left(\left(\sum_{k=2}^{\infty} q^{-k\partial(p)}\left(f(p^{k-1})f(p)-f(p^k)\right)\right)^{\ell}\right. \\
&\qquad - \left.\left(\sum_{k=2}^{\infty} r^{k\partial(p)}\left(f(p^{k-1})f(p)-f(p^k)\right)\right)^{\ell}\right)\Bigg] \\
= &\ o(1),
\end{aligned}
$$

by (3.18). Therefore, we obtain

$$
\begin{aligned}
&\prod_{\partial(p)\leq m}(1-r^{\partial(p)})\left(1+\sum_{k=1}^{\infty} r^{k\partial(p)}f(p^k)\right) \\
&\qquad = \prod_{\partial(p)\leq m}(1-q^{-\partial(p)})\left(1+\sum_{k=1}^{\infty} q^{-k\partial(p)}f(p^k)\right)+o(1). \qquad (3.19)
\end{aligned}
$$

Then (3.14) follows from (3.15), (3.16), (3.17) and (3.19).

Finally, assume that (3.1) converges for $\theta = \alpha \neq 0$. Then, for the multiplicative function $f(a)q^{-i\partial(a)\alpha}$, (3.1) converges for $\theta = 0$. The above argument yields

$$
\begin{aligned}
\sum_{\partial(a)=m} f(a)q^{-i\partial(a)\alpha} &= Aq^m\prod_{\partial(p)\leq m}(1-q^{-\partial(p)})\left(1+\sum_{k=1}^{\infty} q^{-k\partial(p)(1+i\alpha)}f(p^k)\right) \\
&\quad +o(q^m),
\end{aligned}
$$

and then (3.2) follows. □

## 6.4 Mean–Values of Multiplicative Functions

We finally deduce the following theorem on mean–values of multiplicative functions, which is an analogue of the *Halász–Wirsing–Delange theorem* (cf. Halász [1], Wirsing [2], Delange [1], and Elliott [1]).

(6.4.1) THEOREM. (cf. Zhang [8]). *Suppose (i) that $\mathcal{G}$ is a Chebyshev additive arithmetical semigroup satisfying (2.4), or (ii) that (2.14) holds. Let $f$ be a multiplicative function with $|f(a)| \le 1$ for all $a \in \mathcal{G}$. Then the (asymptotic) mean–value*

$$m_f \ (or\ m(f)) = \lim_{n\to\infty} \frac{1}{G(n)} \sum_{\partial(a)=n} f(a)$$

*exists and is non–zero if and only if*

*(i) for each $p$ with $\partial(p) \le \frac{\log 2}{\log q}$,*

$$1 + \sum_{k=1}^{\infty} f(p^k) q^{-k\partial(p)} \ne 0,$$

*and*

*(ii) the series*

$$\sum_p q^{-\partial(p)}(1 - f(p))$$

*converges.*

*Moreover, if (i) and (ii) are satisfied, then*

$$m_f = \prod_p (1 - q^{-\partial(p)}) \left(1 + \sum_{k=1}^{\infty} q^{-k\partial(p)} f(p^k)\right).$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

*Further, the mean–value $m_f$ exists and is zero if and only if either there exist a real number $\alpha$ and a prime $p_0$ with $\partial(p_0) \le \frac{\log 2}{\log q}$ such that the series*

$$\sum_p q^{-\partial(p)} \left(1 - Re(f(p)q^{-i\partial(p)\alpha})\right)$$

*converges, and such that*

$$1 + \sum_{k=1}^{\infty} q^{-k\partial(p_0)(1+i\alpha)} f(p_0^k) = 0,$$

*or the series*

$$\sum_p q^{-\partial(p)} \left(1 - Re(f(p)q^{-i\partial(p)\theta})\right)$$

*diverges for all real numbers $\theta$.*

Proof. If conditions (i) and (ii) hold, then (3.1) converges with $\theta = 0$. Therefore, from (3.2) with $\alpha = 0$ of Theorem 6.3.1, we obtain

$$m_f = \lim_{m\to\infty} \frac{F(m)}{G(m)} = \prod_p (1 - q^{-\partial(p)}) \left(1 + \sum_{k=1}^{\infty} q^{-k\partial(p)} f(p^k)\right),$$

which is non–zero since conditions (i) and (ii) guarantee the non–vanishing of each factor and the convergence of the infinite product. If the condition (iii) holds then, by (3.2), $F(m) = o(q^m)$ and $m_f = 0$. Finally, if the condition (iv) holds then plainly, by Theorem 6.3.1, $m_f = 0$.

Conversely, assume first that $f$ has mean–value $m_f = 0$. Then either (3.1) diverges for all real $\theta$, that is, the condition (iv) holds, or (3.1) converges for $\theta = \alpha$, a real number. In the second case, for the function $g(a) := f(a)q^{-i\alpha\partial(a)}$,

$$\sum_p q^{-\partial(p)}(1 - Re\, g(p))$$

converges and then so does (3.1) with $g$ in place of $f$ and $\theta = 0$. Also,

$$m_g = \lim_{m\to\infty} \frac{1}{G(m)} \sum_{\partial(a)=m} g(a) = \lim_{m\to\infty} q^{-i\alpha m} \frac{F(m)}{G(m)} = 0.$$

Therefore, by (3.2) of Theorem 6.3.1 with $\alpha = 0$ and $g$ in place of $f$, we obtain

$$\lim_{m\to\infty} \prod_{\partial(p)\le m} (1 - q^{-\partial(p)}) \left(1 + \sum_{k=1}^{\infty} q^{-k\partial(p)} g(p^k)\right) = 0;$$

that is,

$$\lim_{m\to\infty} \prod_{\partial(p)\le m} (1 - q^{-\partial(p)}) \left(1 + \sum_{k=1}^{\infty} q^{-k\partial(p)(1+i\alpha)} f(p^k)\right) = 0.$$

Hence there must be a prime $p$ with $\partial(p) \le \frac{\log 2}{\log q}$ such that

$$1 + \sum_{k=1}^{\infty} q^{-k\partial(p)(1+i\alpha)} f(p^k) = 0$$

(if $\partial(p) > \frac{\log 2}{\log q}$, this sum is never zero), i.e., the condition (iii) holds.

Assume then $m_f \ne 0$. Then (2.2) holds with $\alpha = 0$, $L(m) = 1$, and $c = m_f$. Theorem 6.2.2 implies that the generating function

$$\hat{F}(y) = \frac{c}{1 - qy} + o\left(\frac{1}{1 - q|y|}\right)$$

as $|y| \to q^{-1}-$. However,

$$\frac{\hat{F}(y)}{Z(y)} = F_4(y) \exp\left\{- \sum_{\partial(p)\ge \frac{\log 3}{\log q}} y^{\partial(p)}(1 - f(p))\right\},$$

where

$$\begin{aligned} F_4(y) \;&=\; \prod_{\partial(p)<\frac{\log 3}{\log q}} (1 - y^{\partial(p)}) \left(1 + \sum_{k=1}^{\infty} f(p^k) y^{k\partial(p)}\right) \\ &\quad\times \prod_{\partial(p)\ge\frac{\log 3}{\log q}} \left(1 + \sum_{k=1}^{\infty} \left(f(p^k) - f(p^{k-1})f(p)\right) y^{k\partial(p)}\right) \\ &\quad\times \exp\left\{- \sum_{\partial(p)\ge\frac{\log 3}{\log q}} \sum_{k=2}^{\infty} \frac{1}{k} \left(1 - f^k(p)\right) y^{k\partial(p)}\right\} \end{aligned}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

is holomorphic in the disk $\left\{|y| < q^{-\frac{1}{2}}\right\}$. Hence we obtain

$$\begin{aligned}\lim_{r\to q^{-1}-}\frac{\hat{F}(r)}{Z(r)} &= F_4(q^{-1})\lim_{r\to q^{-1}-}\exp\left\{-\sum_{\partial(p)\geq\frac{\log 3}{\log q}} r^{\partial(p)}(1-f(p))\right\}\\ &= \frac{c}{A}=\frac{m_f}{A}\neq 0.\end{aligned}$$

Thus $F_4(q^{-1})\neq 0$, and hence the condition (i) holds. Also,

$$\sum_{\partial(p)\geq\frac{\log 3}{\log q}} r^{\partial(p)}(1-Re\,f(p)) \tag{4.1}$$

must converge, and then

$$\lim_{r\to q^{-1}-}\sum_{\partial(p)\geq\frac{\log 3}{\log q}} r^{\partial(p)}Im\,f(p)$$

does exist. Now

$$\sum_{\partial(p)\geq\frac{\log 3}{\log q}} r^{\partial(p)}Im\,f(p) = \sum_{m\geq\frac{\log 3}{\log q}}\left(\sum_{\partial(p)=m} Im\,f(p)\right)r^m,$$

with

$$\left|\sum_{\partial(p)=m} Im\,f(p)\right| \leq \sum_{\partial(p)=m} 1 = P(m) \ll \frac{q^m}{m}.$$

Hence, by the well-known Littlewood tauberian theorem (cf. Titchmarsh [1]),

$$\sum_{m\geq\frac{\log 3}{\log q}}\left(\sum_{\partial(p)=m} Im\,f(p)\right)q^{-m}$$

is convergent, and then so is

$$\sum_{\partial(p)\geq\frac{\log 3}{\log q}} q^{-\partial(p)}Im\,f(p). \tag{4.2}$$

This implies the condition (ii). Since (4.1) converges, we may also appeal to (3.2) with $\alpha = 0$ and deduce the convergence of (4.2) as in the classical probabilistic number theory (cf. Elliott [1], Vol. I, Chapter 6). □

To conclude our discussion, as a consequence of Theorem 6.4.1, we prove the following alternative mean–value theorem, which is in some ways an analogue of a fine theorem of Wirsing (cf. Wirsing [2], Elliott [1]).

(6.4.2) THEOREM. (cf. Zhang [8]). *Suppose (i) that $\mathcal{G}$ is a Chebyshev additive arithmetical semigroup satisfying (2.4), or (ii) that (2.14) holds. Let $f$ be a multiplicative function such that $|f(a)| \leq 1$ for all $a \in \mathcal{G}$. If there exist a subset $\mathcal{P}_1$ of $\mathcal{P}$ and a number $\varepsilon > 0$ such that*

$$\sum_{p \in \mathcal{P}_1} q^{-\partial(p)} < \infty,$$

*and such that*

$$(Re\, f(p))^2 + (1+\varepsilon)^2 (Im\, f(p))^2 \leq 1 \tag{4.3}$$

*for all $p \notin \mathcal{P}_1$, then*

$$\lim_{m\to\infty} \frac{1}{G(m)} \sum_{\partial(a)=m} f(a), \quad or \quad \lim_{m\to\infty} \frac{(-1)^m}{G(m)} \sum_{\partial(a)=m} f(a), \tag{4.4}$$

*exists.*

*Remark.* Warlimont [4] proved this result under the condition $|Im\, f(p)| \leq K\,(1 - |Re\, f(p)|)$, with $0 \leq K < \frac{1}{\sqrt{3}}$. This condition implies $(Re\, f(p))^2 + K^{-2}(Im\, f(p))^2 \leq 1$. A simple example $f(a) = (-1)^{\partial(a)}$ shows that, under the condition (4.3), $m_f$ does not necessarily exist and therefore the alternative shows substantial divergence from the classical theory. Also, a simple example $f(a) = i^{\partial(a)}$, for which neither limit of (4.4) exists, shows that a condition of the kind of (4.3) is necessary for the truth of the theorem.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

PROOF. By Theorem 6.4.1, if the condition (iii) or the condition (iv) holds, then $m_f = 0$. Therefore we may assume that there exists a real number $\alpha$ such that

$$\sum_p q^{-\partial(p)}\left(1 - Re(f(p)q^{-i\partial(p)\alpha})\right) \tag{4.5}$$

converges. Also we may assume that if (3.1) converges for $\theta = \alpha'$, in particular, $\alpha' = \alpha$, then

$$1 + \sum_{k=1}^{\infty} q^{-k\partial(p)(1+i\alpha')} f(p^k) \neq 0 \tag{4.6}$$

for all $p$ (for $p$ with $\partial(p) > \frac{\log 2}{\log q}$, this is certainly true). From (4.3) and (4.5), we can conclude that

$$\sum_p q^{-\partial(p)}\left(1 - Re(f(p)q^{i\partial(p)\alpha})\right) \tag{4.7}$$

converges. Actually we have, for $p \notin \mathcal{P}_1$,

$$\begin{aligned}&(Re\, f(p))\cos\theta + (1+\varepsilon)(Im\, f(p))\sin\theta \\ &\quad \le \left[(Re\, f(p))^2 + (1+\varepsilon)^2(Im\, f(p))^2\right]^{\frac{1}{2}} \le 1,\end{aligned}$$

and hence

$$\varepsilon(Im\, f(p))\sin(\alpha\partial(p)\log q) \le 1 - Re\left(f(p)q^{-i\alpha\partial(p)}\right).$$

Then the convergence of (4.7) follows from the inequality

$$\begin{aligned}&\sum_{\partial(p)\le M} q^{-\partial(p)}\left(1 - Re(f(p)q^{i\partial(p)\alpha})\right) \\ &= \sum_{\partial(p)\le M} q^{-\partial(p)}\left(1 - Re(f(p)q^{-i\partial(p)\alpha})\right) \\ &\quad +2\sum_{\partial(p)\le M} q^{-\partial(p)}(Im\, f(p))\sin(\partial(p)\alpha\log q) \\ &\le \left(1 + \frac{2}{\varepsilon}\right)\sum_p q^{-\partial(p)}\left(1 - Re(f(p)q^{-i\partial(p)\alpha})\right) + 2\sum_{p\in\mathcal{P}_1} q^{-\partial(p)}.\end{aligned}$$

Now let $g(a) := f(a)q^{-i\partial(a)\alpha}$. From (4.5) and (4.6) with $\alpha' = \alpha$, conditions (i) and (ii) of Theorem 6.4.1 with $g$ in place of $f$ hold. Thus

$$m_g = \lim_{m\to\infty} \frac{1}{G(m)} \sum_{\partial(a)=m} g(a) = \lim_{m\to\infty} \frac{q^{-im\alpha}}{G(m)} \sum_{\partial(a)=m} f(a) \neq 0$$

eixsts. It follows that

$$F(m) = Am_g q^{m(1+i\alpha)} + o(q^m).$$

Similarly, let $h(a) := f(a)q^{i\partial(a)\alpha}$. From (4.7) and (4.6) with $\alpha' = -\alpha$, we conclude that

$$F(m) = Am_h q^{m(1-i\alpha)} + o(q^m).$$

Hence $\alpha \log q = 0$ or $\pi$ mod $2\pi$. If $\alpha = 0$, $m_f = m_g \neq 0$. If $\alpha \log q = \pi$ mod $2\pi$, then

$$\lim_{m\to\infty} \frac{(-1)^m}{G(m)} \sum_{\partial(a)=m} f(a) = m_g \neq 0. \qquad \square$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

## 6.5 Mean–Values of the Functions $\lambda$ and $\mu$

As an application of Theorems 6.4.1 and 6.4.2, combining with Theorem 5.4.1 of Chapter 5, we consider again (asymptotic) mean–values of the Liouville and Möbius functions $\lambda$ and $\mu$ defined on an additive arithmetical semigroup $\mathcal{G}$ (cf. Lemma 4.1.2 of Chapter 4 for the "classical" case).

(6.5.1) THEOREM. (cf. Zhang [7]). *Assume that*

$$G(m) = Aq^m + O\left(q^m m^{-\gamma}\right) \tag{5.1}$$

*holds, with constants $A > 0$ and $\gamma > 2$. Then*

$$\sum_{\partial(a)=m} \lambda(a) = o(q^m), \qquad \sum_{\partial(a)=m} \mu(a) = o(q^m)$$

*if the generating function $Z(y)$ of $\mathcal{G}$ has no zeros on the circle $\{|y| = q^{-1}\}$; otherwise,*

$$\lim_{m\to\infty} \frac{(-1)^m}{G(m)} \sum_{\partial(a)=m} \lambda(a), \quad \lim_{m\to\infty} \frac{(-1)^m}{G(m)} \sum_{\partial(a)=m} \mu(a)$$

*exist, if $Z(y)$ has a zero at $y = -q^{-1}$.*

*Remark.* The mean–value of $\mu$ is also considered by Warlimont [4], and Indlekofer and Manstavicius [1]. If $Z(y)$ has a zero at $y = -q^{-1}$, then the order of the zero is one and $Z(y)$ has no other zeros on the closed disk $\{|y| \leq q^{-1}\}$, as we know from Corollary 5.3.4 of Chapter 5. In this case, $\mu$ does not have a mean–value because of the dominant perturbation of the zero at $y = -q^{-1}$; instead, it has alternative mean–values by Theorem 6.4.2. This is well illustrated by Example 3.8.1 of Chapter 3, as we shall see from a brief discussion given at the end of this section. We note that this phenomenon does not occur in the theory of Beurling's generalized integers (cf. Zhang [9]).

PROOF. As in classical number theory, we have

$$\begin{aligned}
&Z^3(r)\left|Z^4(re^{i\theta})\right|\left|Z(re^{i2\theta})\right| \\
&= \prod_{m=1}^{\infty}\left[(1-r^m)^3|1-r^m e^{im\theta}|^4|1-r^m e^{i2m\theta}|\right]^{-P(m)} \\
&= \exp\left\{\sum_{m=1}^{\infty}P(m)\sum_{k=1}^{\infty}\frac{r^{km}}{k}(3+4\cos km\theta+\cos 2km\theta)\right\} \\
&\geq 1,
\end{aligned}$$

for $0 \leq r < q^{-1}$ and all $\theta \in \mathbb{R}$, since $3+4\cos km\theta+\cos 2km\theta \geq 0$ (see Section 3.5). Note that, for $\theta \neq (2n+1)\pi$, $n \in \mathbb{Z}$, $\lim_{r\to q^{-1}-}\left|Z(re^{2i\theta})\right|$ exists and is finite. Hence, for $\theta \neq (2n+1)\pi$, $n \in \mathbb{Z}$,

$$Z(r)\left|Z(re^{i\theta})\right| \to \infty,$$

or, equivalently,

$$\log\left(Z(r)\left|Z(re^{i\theta})\right|\right) \to \infty$$

as $r \to q^{-1}-$. We note that

$$\begin{aligned}
\log\left(Z(r)\left|Z(re^{i\theta})\right|\right) &= \sum_{m=1}^{\infty}P(m)\sum_{k=1}^{\infty}\frac{r^{km}}{k}(1+Re\, e^{ikm\theta}) \\
&= \sum_{m=1}^{\infty}P(m)r^m(1+Re\, e^{im\theta})+o(1),
\end{aligned}$$

since $P(m) \ll q^m m^{-1}$. Therefore we have

$$\sum_{m=1}^{\infty}P(m)r^m(1+Re\, e^{im\theta}) \to \infty$$

as $r \to q^{-1}-$ for all $\theta \neq (2n+1)\pi$, $n \in \mathbb{Z}$. If we now take $f=\lambda$ or $f=\mu$ in Theorem 6.4.1, then we find that

$$\begin{aligned}
S: &= \sum_p q^{-\partial(p)}\left(1-Re(f(p)q^{-i\theta\partial(p)})\right) \\
&= \lim_{r\to q^{-1}-}\sum_{m=1}^{\infty}P(m)r^m(1+Re\, e^{-im\theta\log q}) \\
&= \infty
\end{aligned}$$

holds for all $\theta \in \mathbb{R}$ and $\theta \neq \frac{(2n+1)\pi}{\log q}$, $n \in \mathbb{Z}$, because $f(p) = -1$.

For $\theta = \frac{(2n+1)\pi}{\log q}$,

$$\begin{aligned} S &= \sum_{m=1}^{\infty} P(m) q^{-m}(1 + Re\, e^{-im(2n+1)\pi}) \\ &= 2\sum_{m=1}^{\infty} P(2m) q^{-2m}. \end{aligned}$$

Assuming (5.1) with $\gamma > 2$, by Theorem 5.4.1 of Chapter 5, we have

$$S = \sum_{m=1}^{\infty} \frac{1}{m}\left(1 + O(m^{-\gamma+1})\right) = \infty$$

if $Z(y)$ has no zeros at $y = -q^{-1}$, since

$$P(n) = \frac{1}{n}\sum_{r|n} \mu(r)\bar{\Lambda}\left(\frac{n}{r}\right)$$

(*here* $\mu$ is the *classical* Möbius function). Hence $S$ diverges for all real numbers $\theta$, and

$$\sum_{\partial(a)=m} f(a) = o(q^m) \tag{5.2}$$

by Theorem 6.4.1, if $Z(y)$ has no zeros at $y = -q^{-1}$. Now assume that $Z(y)$ has a zero at $y = -q^{-1}$. Then, by Theorem 5.4.1 of Chapter 5,

$$S = \sum_{m=1}^{\infty} \frac{1}{m} O(m^{-\gamma+2})$$

converges for $\alpha = \frac{(2n+1)\pi}{\log q}$, $n \in \mathbb{Z}$. In this case, $f$ does not have mean–value 0 (by Theorem 6.4.1). Actually, if $f = \lambda$ then, for each $p$, we have

$$\begin{aligned} 1 + \sum_{k=1}^{\infty} q^{-k\partial(p)(1+i\alpha)} f(p^k) &= 1 + \sum_{k=1}^{\infty} q^{-k\partial(p)}(-1)^{k\left(\partial(p)+1\right)} \\ &= \frac{1}{1 - (-1)^{\partial(p)+1} q^{-\partial(p)}} > 0, \end{aligned}$$

and, if $f = \mu$ then we have

$$1 + \sum_{k=1}^{\infty} q^{-k\partial(p)(1+i\alpha)} f(p^k) = 1 - (-1)^{\partial(p)} q^{-\partial(p)} > 0,$$

since $q > 1$, $\partial(p) \geq 1$. It remains to determine whether $f$ has a non–zero mean–value. We have

$$\begin{aligned}\sum_p q^{-\partial(p)}(1 - f(p)) &= 2\sum_{m=1}^{\infty} P(m)q^{-m} \geq 2\sum_{m=1}^{\infty} P(2m-1)q^{-2m+1} \\ &= \infty,\end{aligned}$$

by Theorem 5.4.1 of Chapter 5. Therefore, by Theorem 6.4.1, $f$ does not have a non–zero mean–value and the mean–value $m_f$ does not exist if $Z(y)$ has a zero at $y = -q^{-1}$. Then Theorem 6.4.2 implies that

$$\lim_{m\to\infty} \frac{(-1)^m}{G(m)} \sum_{\partial(a)=m} f(a)$$

exists. □

Theorem 6.5.1 is well illustrated by Example 3.8.1 of Chapter 3. Consider the additive arithmetical semigroup $\mathcal{G}$ defined there. Then the generating function of $\mu$ or its summatory function is

$$M(y) := \sum_{a\in\mathcal{G}} \mu(a)y^{\partial(a)} = \sum_{m=0}^{\infty} \left( \sum_{\partial(a)=m} \mu(a) \right) y^m, \quad |y| < q^{-1}.$$

It is easily seen that

$$\begin{aligned} M(y) &= \prod_p (1 - y^{\partial(p)}) = \prod_{m=1}^{\infty} (1 - y^m)^{P(m)} \\ &= \frac{1}{Z(y)} = \frac{1 - qy}{1 + qy} \left( \frac{1 - qy^2}{1 + qy^2} \right)^{\frac{1}{2}} e^{-F(y)}, \end{aligned}$$

which is meromorphic in the domain $\mathcal{D} \cap \left\{ |y| < q^{-\frac{1}{3}} \right\}$. Here the domain $\mathcal{D}$ is formed by cutting the complex plane along the real axis from $-\infty$ to

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

$-q^{-\frac{1}{2}}$, and from $q^{-\frac{1}{2}}$ to $+\infty$, and along the imaginary axis from $-i\infty$ to $-iq^{-\frac{1}{2}}$, and from $iq^{-\frac{1}{2}}$ to $i\infty$. Also, here the function $F(y)$ is holomorphic in the disk $\left\{|y| < q^{-\frac{1}{3}}\right\}$, and the function

$$H_1(y) := \left(\frac{1 - qy^2}{1 + qy^2}\right)^{\frac{1}{2}}$$

is the single–valued branch with $H_1(0) = 1$ of the associated multiple–valued function in $\mathcal{D}$. Therefore we have

$$\sum_{\partial(a)=m} \mu(a) = \frac{1}{2\pi i}\int_{|y|=r} \frac{M(y)}{y^{m+1}}\, dy$$

where $0 < r < q^{-1}$. If we shift the integration contour to the circle $|y| = q^{-\frac{1}{2}-\varepsilon}$, then we obtain

$$\begin{aligned}\sum_{\partial(a)=m} \mu(a) &= \operatorname*{Res}_{y=-q^{-1}} \frac{M(y)}{y^{m+1}} + \frac{1}{2\pi i}\int_{|y|=q^{-\frac{1}{2}-\epsilon}} \frac{M(y)}{y^{m+1}}\, dy \\ &= (-1)^{m+1} 2q^m \left(\frac{q-1}{q+1}\right)^{\frac{1}{2}} e^{-F\left(-q^{-1}\right)} + O_\varepsilon\left(q^{\left(\frac{1}{2}+\varepsilon\right)m}\right).\end{aligned}$$

Therefore

$$\lim_{m\to\infty} \frac{(-1)^m}{G(m)} \sum_{\partial(a)=m} \mu(a) = -2\left(\frac{q-1}{q+1}\right)^{\frac{1}{2}} e^{-F\left(-q^{-1}\right)}.$$

Hence $\mu$ does not have a mean–value here, because of the dominant perturbation of the zero of $Z(y)$ at $y = -q^{-1}$.

## 6.6 Mean–Value Theorems for Beurling–Type Semigroups

Some theorems in previous sections have also been proved for *Beurling–type* additive arithmetical semigroups (see Section 5.5), with the following condition (6.3) in place of (2.4), and the condition (6.6) in place of (2.14), etc. In particular, we now state the following two theorems without including proofs, which correspond to Theorem 6.2.1 and Theorem 6.5.1 respectively. Readers with interest in proofs may read Zhang [7,8].

(6.6.1) THEOREM. *Suppose there exist a constant $c$, real constants $\alpha, \tau > 0$, and $q > 1$, and a measurable, slowly oscillating function $L(x)$ with $|L(x)| = 1$, such that*

$$F(m) = \frac{cq^{m(1+i\alpha)}m^{\tau-1}}{\Gamma(\tau)}L(m) + o\left(q^m m^{\tau-1}\right) \qquad (6.1)$$

*as $m \to \infty$. Then the asymptotic formula*

$$\hat{F}(y) = \frac{c}{(1-q^{1+i\alpha}y)^\tau}L\left(\frac{1}{1-q|y|}\right) + o\left(\frac{1}{(1-q|y|)^\tau}\right) \qquad (6.2)$$

*holds as $|y| \to q^{-1}-$.*

*Conversely, let $\rho_1 < \cdots < \rho_r$ be constants such that $\rho_r = \tau \geq 1$, and $A_1, \ldots, A_r$ be real constants such that $A_r = A > 0$. Set*

$$Q(n) = \sum_{\nu=1}^{r} A_\nu n^{\rho_\nu - 1}.$$

*Suppose that*

$$\sum_{n=1}^{\infty} \left|G(n)q^{-n} - Q(n)\right| < \infty, \qquad (6.3)$$

*and either*

$$G(n)q^{-n} - Q(n) = O(n^{-1}), \qquad (6.4)$$

*or*

$$\sum_{n=1}^{\infty} n\left(G(n)q^{-n} - Q(n)\right)^2 < \infty. \tag{6.5}$$

*Moreover, suppose* $|f(a)| \le 1$ *for all* $a \in \mathcal{G}$, *and either*

*(i)* $f$ *is a completely multiplicative function on* $\mathcal{G}$, *or*

*(ii)* $f$ *is a multiplicative function such that, for each prime* $p$ *with* $\partial(p) < \frac{\log 2}{\log q}$, *there exists a positive integer* $k(p)$ *such that* $q^{\partial(p)} - 1 - q^{-\left(k(p)-1\right)\partial(p)} \ge 0$, *and* $f(p^k) = 0$ *for all* $1 \le k < k(p)$.

*Then (6.2) implies (6.1).*

*Note.* If we assume

$$\sum_{n=1}^{\infty} \sup_{n \le m} \left|G(m)q^{-m} - Q(m)\right| < \infty, \tag{6.6}$$

or, in particular, assume

$$G(m) = q^m \sum_{\nu=1}^{r} A_\nu m^{\rho_\nu - 1} + O\left(q^m m^{-\gamma}\right) \tag{6.7}$$

with $\gamma > 1$, then (6.3) and (6.4) hold.

(6.6.2) Theorem. *Assume (6.7) with* $q > 1$ *and* $\gamma > \max\{2 + \rho_r, 3\}$. *Then*

$$\sum_{\partial(a)=m} \lambda(a) = o\left(q^m m^{\rho_r - 1}\right),$$

*and*

$$\sum_{\partial(a)=m} \mu(a) = o\left(q^m m^{\rho_r - 1}\right),$$

*if* $Z(y)$ *has no zeros at* $y = -q^{-1}$ *or a zero at* $y = -q^{-1}$ *of order less then* $\rho_r$; *otherwise both*

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

$$\lim_{m\to\infty} \frac{(-1)^m}{G(m)} \sum_{\partial(a)=m} \lambda(a), \quad \lim_{m\to\infty} \frac{(-1)^m}{G(m)} \sum_{\partial(a)=m} \mu(a)$$

*exist.*

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

# CHAPTER 7

# BASICS OF PROBABILISTIC NUMBER THEORY FOR SEMIGROUPS

## 7.1 Necessary Results from Theory of Probability

In this chapter we shall investigate the limit distributions of real–valued additive functions on (additive) arithmetical semigroups. Especially, we shall prove an analogue of the well–known Lindeberg–Feller *central limit theorem*, and an analogue of the celebrated *Erdős–Kac theorem*. Since the probabilistic theory of (additive) arithmetical semigroups is still developing and new results are still being published, we shall confine ourselves here to basics of the theory. For readers with interest in the classical background of theorems in this chapter, we refer to Elliott's monograph [1].

Several authors have made contributions to this subject, e.g. Indlekofer and Manstavicius [1], and Zhang [3]. The discussion given in this chapter follows mainly the paper [3] by Zhang.

In the following discussions, as in the classical probabilistic number theory, a theorem is usually formulated in the fashion of probability theory, the basic idea of a proof of the theorem is illustrated by a proper probability model, and then the proof appeals to relevant theorems in probability theory. Hence some familiarity with the basics of the theory of convergence of distributions in probability theory is a *prerequisite* below, although, in

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

this section first, *we also give a brief survey* of certain relevant concepts and necessary results, which are well-known and may be found in standard references in probability theory (e.g. Gnedenko and Kolmogorov [1], and Billingsley [1]). We shall state such results without proofs.

### 7.1.1 The Chebyshev inequality and other initial results

Let $(\Omega, \mathcal{F}, P)$ be a probability space, that is, $\mathcal{F}$ is a $\sigma$-field of subsets of the sample space $\Omega$ and $P$ is a probability measure on $\mathcal{F}$. The members of $\mathcal{F}$ are called *measurable* sets. A *random variable* on $(\Omega, \mathcal{F}, P)$ is a real-valued function $X(\omega)$ which is defined for $\omega \in \Omega$ and measurable on $\mathcal{F}$.

Then for each one-dimensional real Borel set $A$, the event $[X \in A] = \{\omega : X(\omega) \in A\}$ is measurable; especially, so is $[X \leq x]$ for each real number $x$. The *distribution* or *law* of $X$ is the probability measure

$$\mu(A) = P[X \in A]$$

defined on the $\sigma$-field of one-dimensional Borel sets. The *distribution function* of $X$ is the function

$$F(x) := \mu(-\infty, x] = P[X \leq x]$$

defined for real $x$. Hence $F(x)$ is non-decreasing and right-continuous. Moreover

$$\lim_{x \to -\infty} F(x) = 0, \quad \lim_{x \to +\infty} F(x) = 1.$$

Conversely, any real-valued function $F(x)$ with these properties is the distribution function of a random variable on some probability space.

The distribution functions most commonly used are determined by a finite number of parameters. Among these parameters are the *mean* (or *expectation*) $EX$ and the *variance* $Var\, X$ of a random variable $X$, which are respectively defined by

$$EX = \int_{-\infty}^{\infty} x dF(x),$$

and

$$Var\, X = E(X - EX)^2 = \int_{-\infty}^{\infty} (x - EX)^2 dF(x),$$

where $F(x)$ is the distribution function of $X$. The variance can also be written in the form

$$Var\, X = E(X^2) - (EX)^2.$$

(7.1.1) LEMMA. (The Chebyshev inequaltiy)

$$E[\,|X| \geq a\,] \leq \frac{E(X^2)}{a^2}$$

*for any* $a > 0$.

The idea of this well-known inequality has proved of the greatest importance in probability and statistics.

For any random variables $X_j$, $j = 1, \ldots, n$, on the same probability space $\Omega$,

$$E(X_1 + \cdots + X_n) = EX_1 + \cdots + EX_n.$$

If $X_j$, $j = 1, \ldots, n$ are *independent*, i.e.,

$$P[X_1 \leq x_1, \ldots, X_n \leq x_n] = P[X_1 \leq x_1] P[X_2 \leq x_2] \cdots P[X_n \leq x_n]$$

for all $x_1, \ldots, x_n$, then

$$Var(X_1 + \cdots + X_n) = Var\, X_1 + \cdots + Var\, X_n.$$

To prove our main theorems in Section 7.6 below, we need the following existence theorem for independent sequences of random variables.

(7.1.2) LEMMA. *If $\mu_n$, $n = 1, 2, \ldots$, is a finite or infinite sequence of probability measures on the $\sigma$-field of one-dimensional Borel sets, then there exists on some probability space $(\Omega, \mathcal{F}, P)$ an independent sequence $X_n$, $n = 1, 2, \ldots$, of random variables such that $X_n$ has distribution $\mu_n$.*

For a proof of this existence theorem, we refer to Billingsley [1], Chapter 4, Theorem 20.4.

Let $X$ and $Y$ be independent random variables, with respective distribution functions $F(x)$ and $G(x)$. Then $X+Y$ has the distribution function

$$H(y) = \int_{-\infty}^{\infty} G(y-x)dF(x),$$

which is called the *convolution* of $F(x)$ and $G(x)$, denoted by $F * G$. This convolution operation is commutative and associative.

### 7.1.2 Weak convergence, characteristic functions, and the continuity theorem

If $F_n(x)$ and $F(x)$ are distribution functions, and if

$$\lim_{n\to\infty} F_n(x) = F(x)$$

holds for each $x$ at which $F(x)$ is continuous, then we say that $F_n$ *converges weakly* to $F$ as $n \to \infty$, and write $F_n \Longrightarrow F$. Sometimes $F(x)$ will then be referred to as the *limit distribution* or *limit law.* In this case, if $F_n$ and $F$ are distribution functions of random variables $X_n$ and $X$ respectively, we also say that $X_n$ *converges in distribution* or *in law* to $X$, and write $X_n \Longrightarrow X$.

Associated with a distribution function $F(x)$ is the *characteristic* function, defined by

$$\phi(t) = \int_{-\infty}^{\infty} e^{itx} dF(x),$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

the Fourier transform of $F(x)$. This characteristic function is defined for all real values of $t$. It is uniformly continuous for $-\infty < t < \infty$ and satisfies

$$\phi(0) = 1, \quad |\phi(t)| \leq 1.$$

The characteristic function $\phi(t)$ contains all information about the distribution function $F(x)$, because $\phi$ uniquely determines the function it comes from. This fundamental fact is a consequence of an *inversion formula* given as follows.

(7.1.3) LEMMA. (Inversion formula) *Let $u$ and $v$ be continuity points of $F(x)$, and let $\phi(t)$ be the characteristic function of $F(x)$. Then*

$$F(u) - F(v) = \lim_{T \to \infty} \frac{1}{2\pi} \int_{-T}^{T} \frac{e^{-itv} - e^{-itu}}{it} \phi(t) dt.$$

Weak convergence of distribution functions can be formulated in terms of characteristic functions, as follows:

(7.1.4) LEMMA. (Continuity theorem) *Let $\phi_n(t)$ be the characteristic function of the distribution function $F_n(x)$, $n = 1, 2, \ldots$. Then the following propositions are equivalent:*

*(i) The distribution functions $F_n(x)$ converge weakly to a distribution function $F(x)$ as $n \to \infty$.*

*(ii) There exists a function $\phi(t)$ defined for $-\infty < t < \infty$ such that $\phi(t)$ is continuous at $t = 0$ and $\lim_{n\to\infty} \phi_n(t) = \phi(t)$, $-\infty < t < \infty$.*

*(iii) There exists a function $\phi(t)$ defined for $-\infty < t < \infty$ such that $\lim_{n\to\infty} \phi_n(t) = \phi(t)$ uniformly on every finite interval of $t$.*

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

In cases (ii) and (iii), $\phi(t)$ will be the characteristic function of some distribution function $F(x)$, and $F_n(x) \Longrightarrow F(x)$ as $n \to \infty$.

For a proof of this important theorem, we refer to either Gnedenko and Kolmogorov [1], Chapter 2, Theorems 1 and 2, or Billingsley [1], Chapter 5, Section 26.

In investigating weak convergence of distribution functions, the following theorem, sometimes called the *Slutsky theorem*, is also useful.

(7.1.5) LEMMA. *If $X_n$ converges in distribution to $X$, and if $Y_n$ converges in distribution to a constant $c_0$, then*

*(i) $X_n + Y_n$ converges in distribution to $X + c_0$, and*

*(ii) $X_nY_n$ converges in distribution to $c_0X$.*

We refer to Parzen [1] for this result. It is also implied by the remark following Lemma 1.7 in Elliott [1].

### 7.1.3 The central limit theorem and the Kolmogorov theorem

A normal distribution function is

$$\frac{1}{\sigma\sqrt{2\pi}}\int_{-\infty}^{x} e^{-\frac{(u-\mu)^2}{2\sigma^2}}du,$$

where $\mu$ is the mean and $\sigma^2$ is the variance. A random variable is said to be normally distributed if it has normal distribution function.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

In particular, the standard normal distribution function is

$$\Phi(x) = \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-\frac{u^2}{2}} du.$$

Let $N$ denote a random variable which has distribution function $\Phi(x)$. Then $EN = 0$ and $Var\, N = 1$.

The central limit theorem states roughly that the sum of many independent random variables will be approximately normally distributed if each summand has high probability of being small. Suppose that for each positive integer $n$, random variables

$$X_{n1}, X_{n2}, \ldots, X_{nk_n}$$

are independent; the probability space for the sequence may change with $n$.

(7.1.6) LEMMA. (The Lindeberg–Feller central limit theorem) *Suppose*

$$E[X_{nk}] = 0, \quad \sigma_{nk}^2 = E[X_{nk}^2], \ k = 1, \ldots, k_n.$$

*Let* $S_n = X_{n1} + \cdots + X_{nk_n}$, *and* $s_n^2 = \sum_{k=1}^{k_n} \sigma_{nk}^2$. *If the Lindeberg condition*

$$\lim_{n\to\infty} \frac{1}{s_n^2} \sum_{k=1}^{k_n} \int_{|X_{nk}| \geq \varepsilon s_n} X_{nk}^2 dP = 0 \tag{1.1}$$

*holds for each* $\varepsilon > 0$, *then* $S_n/s_n \Longrightarrow N$.

*Conversely, if* $S_n/s_n \Longrightarrow N$, *and*

$$\max_{1\leq k\leq k_n} P\left[\left|\frac{X_{nk}}{s_n}\right| \geq \varepsilon\right] \to 0, \tag{1.2}$$

*(especially,*

$$\max_{1\leq k\leq k_n} \frac{\sigma_{nk}^2}{s_n^2} \to 0)$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

*holds for each $\varepsilon > 0$, then (1.1) is satisfied.*

For proofs of this famous theorem, we refer to Gnedenko and Kolmogorov [1], Chapter 4, Theorems 3 and 4, or Billingsley [1], Chapter 5, Theorems 27.2 and 27.4.

The standard normal distribution is a particular case of infinitely divisible distributions. A distribution function $F$ is said to be *infinitely divisible* if and only if for each positive integer $n$ there exists a distribution function $F_n$ such that $F$ is the $n$-fold convolution $F_n * \cdots * F_n$ ($n$ copies) of $F_n$.

If the associated characteristic functions of distribution functions $F$ and $G$ are $\phi(t)$ and $\psi(t)$ respectively, then the characteristic function of the convolution $F * G$ is $\phi(t)\psi(t)$.

In terms of characteristic functions, if $\phi(t)$ denotes the characteristic function of an infinitely divisible distribution function $F$, then for each positive integer $n$, there will be a characteristic function $\phi_n(t)$ such that $\phi(t) = (\phi_n(t))^n$ for $-\infty < t < \infty$. If the distribution function $F(x)$ of a random variable $X$ is infinitely divisible, we also say that $X$ is *infinitely divisible.*

(7.1.7) LEMMA. (The Kolmogorov theorem) *A distribution function with mean 0 and finite variance $\sigma^2$ is infinitely divisible if and only if its characteristic function $\phi(t)$ is of the form*

$$\phi(t) = \exp\left\{\int_{-\infty}^{\infty} (e^{itu} - 1 - itu)\frac{1}{u^2} dK(u)\right\},$$

*where $K(u)$ is a non-decreasing and right-continuous function and $K(\infty) - K(-\infty)$ is finite.*

*Remark.* Actually, $K(\infty) - K(-\infty) = \sigma^2$.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

For proofs, we refer to Gnedenko and Kolmogorov [1], Chapter 3, or Billingsley [1], Chapter 5, Theorems 28.1, 28.2, and 28.3.

Let $K_n(x)$ and $K(x)$ be non-decreasing and right-continuous functions defined for $-\infty < x < \infty$, such that $\lim_{x\to-\infty} K_n(x) = 0$, $\lim_{x\to-\infty} K(x) = 0$, and $\lim_{x\to\infty} K_n(x)$ and $\lim_{x\to\infty} K(x)$ are finite. If

$$\lim_{n\to\infty} K_n(x) = K(x)$$

holds for each $x$ at which $K(x)$ is continuous, then we say that $K_n(x)$ *converges vaguely* to $K(x)$. If $K_n(x)$ and $K(x)$ are distribution functions, then the vague convergence and the weak convergence are *equivalent.*

(7.1.8) LEMMA. *Let $F_n(x)$ be a sequence of infinitely divisible distribution functions with mean zero, and uniformly bounded variances. Let the characteristic function of $F_n(x)$ be*

$$\exp\left\{\int_{-\infty}^{\infty} (e^{itu} - 1 - itu)u^{-2} dK_n(u)\right\}.$$

*Then $F_n(x)$ converges weakly to a distribution function $F(x)$ if and only if $F(x)$ is infinitely divisible and $K_n(u)$ converges vaguely to $K(u)$ as $n \to \infty$, where the characteristic function of $F(x)$ is*

$$\exp\left\{\int_{-\infty}^{\infty} (e^{itu} - 1 - itu)u^{-2} dK(u)\right\}.$$

For proofs, see Gnedenko and Kolmogorov [1], Chapter 3, Theorem 3, or Billingsley [1], Chapter 5, Theorem 28.4.

### 7.1.4 A finite probability space

Let $f$ be a complex-valued function defined on an arithmetical semigroup $(\mathcal{G}, \partial)$, not identically zero. Recall that $f$ is said to be *additive* if and only

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

if $f(ab) = f(a) + f(b)$ holds for each pair of coprime $a$, $b \in \mathcal{G}$. An additive function $f$ is said further to be **strongly** additive if and only if $f(p^k) = f(p)$ for each prime power $p^k$ with $k \geq 1$; this condition should not be confused with *complete* addivity, when $f(ab) = f(a) + f(b)$ for *all* $a$, $b \in \mathcal{G}$.

Now, consider a real–valued additive function $f$. For a positive integer $m$ and a real number $x$, write

$$\nu_m(f,x) := \sum_{\substack{\partial(a)=m \\ f(a)\leq x}} 1.$$

If there exists a distribution function $F(x)$ such that

$$\frac{\nu_m(f,x)}{G(m)} \Longrightarrow F(x) \tag{1.3}$$

as $m \to \infty$, then we say that $f$ *has the limit distribution* function $F(x)$.

The function $\nu_m(f,x)/G(m)$ of $x$ is a distribution function on a natural probability model: Let $\Omega := \{a : \ a \in \mathcal{G},\ \partial(a) = m\}$, which is a finite set of $G(m)$ elements. The "local" function $f_m(a) := f(a)$ for $a \in \Omega$ assumes only a finite number of values, $\{x_1, x_2, \ldots, x_t\}$, say. The subsets $A_i := \{a : \ a \in \Omega,\ f_m(a) = x_i\}$, $i = 1, \ldots, t$, of $\Omega$ are pairwise disjoint and form a partition of $\Omega$. The ($\sigma$–) field $\mathcal{F}$ generated by this partition consists of unions of a finite number of subsets $A_i$. For $A \in \mathcal{F}$, let $\nu(A) = |A|/G(m)$, where $|A|$ denotes the number of $a \in A$, or the cardinality of $A$. Then $\nu$ is a probability measure on $\mathcal{F}$, and $(\Omega, \mathcal{F}, \nu)$ is a finite probability space. (In Section 7.5, we shall consider a "finer" probability space). Now $f_m$ is measurable on $\mathcal{F}$, and hence a random variable on $(\Omega, \mathcal{F}, \nu)$. The distribution function of $f_m$ is

$$\begin{aligned} \nu[f_m \leq x] &= (G(m))^{-1}\Big|\{a : \ a \in \Omega,\ f_m(a) \leq x\}\Big| \\ &= \frac{\nu_m(f,x)}{G(m)}, \end{aligned} \tag{1.4}$$

the relative frequency of the "event" $[f_m \le x]$.

We may also define a limit distribution function $F(x)$ by

$$\frac{1}{\gamma(m)} \sum_{\substack{\partial(a)\le m\\ f(a)\le x}} 1 \Longrightarrow F(x), \tag{1.5}$$

where $\gamma(m) = \sum_{n\le m} G(n)$ is the total number of elements of degree $n \le m$ in $\mathcal{G}$. However, $F(x)$ is a limit distribution function in the sense (1.5) if and only if it is one in the sense of (1.3). This is a consequence of the following well-known case of the Cesaro theorem and an inverse of this case not known in literature.

(7.1.9) LEMMA. *Let $a_n$, $n = 1, 2, \dots$ and $b_n$, $n = 1, 2, \dots$ be two sequences of real numbers such that $b_n > 0$ and $\sum_{n=1}^{\infty} b_n = \infty$.*

*(1) If $\lim_{n\to\infty} a_n/b_n = s$ then*

$$\lim_{n\to\infty} \frac{a_1 + a_2 + \cdots + a_n}{b_1 + b_2 + \cdots + b_n} = s. \tag{1.6}$$

*(2) Conversely, if (1.6) exists and if $\sum_{n=1}^{m} b_n \ll b_m$ then $\lim_{n\to\infty} a_n/b_n = s$.*

PROOF. A proof of (1) is well-known in Pólya and Szegő [1].

To prove (2), let $\sum_{n=1}^{m} b_n \le K b_m$, where $K$ is a positive constant. Given $\epsilon > 0$, for $m$ sufficiently large,

$$s - \varepsilon < \frac{a_1 + a_2 + \cdots + a_m}{b_1 + b_2 + \cdots + b_m} < s + \varepsilon.$$

Hence

$$\begin{aligned} a_{m+1} &= \sum_{n=1}^{m+1} a_n - \sum_{n=1}^{m} a_n < (s+\varepsilon)\sum_{n=1}^{m+1} b_n - (s-\varepsilon)\sum_{n=1}^{m} b_n \\ &< s b_{m+1} + 2\varepsilon \sum_{n=1}^{m+1} b_n \end{aligned}$$

and similarly

$$sb_{m+1} - 2\varepsilon \sum_{n=1}^{m+1} b_n < a_{m+1}.$$

It follows that

$$s - 2\varepsilon K < \frac{a_{m+1}}{b_{m+1}} < s + 2\varepsilon K,$$

i.e.,

$$\lim_{m\to\infty} \frac{a_m}{b_m} = s. \qquad \square$$

Now let $F(x)$ be a limit distribution function in the sense of (1.3). If we take $a_n = \nu_n(f, x)$ and $b_n = G(n)$, then $a_n/b_n$ converges to $F(x)$ at each point of continuity of $F(x)$. The left-hand side of (1.5) equals

$$\begin{aligned} \frac{1}{\gamma(m)} \sum_{n\le m} \sum_{\substack{\partial(a)=n \\ f(a)\le x}} 1 &= \sum_{n\le m} \nu_n(f,x) \Big/ \sum_{n\le m} G(n) \\ &= \frac{a_0 + a_1 + \cdots + a_m}{b_0 + b_1 + \cdots + b_m} \end{aligned}$$

and, by (1) of Lemma 7.1.9, converges to $F(x)$ at each point of continuity of $F(x)$, i.e., $F(x)$ is also a limit distribution function in the sense (1.5). Conversely, if we assume $G(n) = Aq^n + o(q^n)$ with $A > 0$ and $q > 1$ then $\sum_{n\le m} G(n) \ll G(m)$. In a similar way, by (2) of Lemma 7.1.9, a limit distribution function $F(x)$ in the sense (1.5) is also one in the sense of (1.3).

In this monograph, we consider the limit distribution function $F(x)$ in the sense of (1.3).

The mean of $f_m$ is

$$\begin{aligned} \sum_{i=1}^{t} x_i \nu(A_i) &= \frac{1}{G(m)} \sum_{i=1}^{t} x_i \Big| \{a : \partial(a) = m,\ f(a) = x_i\} \Big| \\ &= \frac{1}{G(m)} \sum_{\partial(a)=m} f(a) \end{aligned}$$

and the variance of $f_m$ is

$$\begin{aligned}\sum_{i=1}^{t} x_i^2\nu(A_i) - \left(\frac{1}{G(m)}\sum_{\partial(a)=m} f(a)\right)^2 \\ = \frac{1}{G(m)}\sum_{\partial(a)=m} f^2(a) - \frac{1}{G^2(m)}\left(\sum_{\partial(a)=m} f(a)\right)^2.\end{aligned}$$

We are mainly interested in additive functions. Assume that

$$G(m) = Aq^m + O(q^m m^{-\gamma}), \quad m \ge 1$$

holds with $A > 0$, $q > 1$, and $\gamma > 1$. If $f$ is additive, then

$$\sum_{\partial(a)=m} f(a) = \sum_{\partial(a)=m}\sum_{p^k\|a} f(p^k) = \sum_{k\partial(p)\le m} f(p^k) \sum_{\substack{\partial(a)=m \\ p^k\|a}} 1.$$

It will be shown in Lemma 7.3.3 that the inner sum on the right–hand side equals

$$Aq^{m-k\partial(p)}\left(1 - q^{-\partial(p)}\right) + O\left(\frac{q^{m-k\partial(p)}}{(m-k\partial(p))^{\gamma}}\right)$$

for $k\partial(p) < m$. Hence

$$\begin{aligned}\sum_{\partial(a)=m} f(a) &= Aq^m\left[\sum_{k\partial(p)\le m} f(p^k)q^{-k\partial(p)}\left(1-q^{-\partial(p)}\right)\right. \\ &\quad \left. +O\left(\sum_{k\partial(p)<m} |f(p^k)|q^{-k\partial(p)}(m-k\partial(p))^{-\gamma}\right)\right] \\ &\quad + \sum_{k\partial(p)=m} f(p^k)\left(1 - A(1-q^{-\partial(p)})\right).\end{aligned}$$

Under further conditions on $f$, as we did in the proofs of (3.13) and (3.14) on $\omega(a)$ and $\Omega(a)$ in Chapter 3, we can write the mean

$$\frac{1}{G(m)}\sum_{\partial(a)=m} f(a) = \sum_{k\partial(p)\le m} f(p^k)q^{-k\partial(p)}\left(1-q^{-\partial(p)}\right) + R_m, \tag{1.7}$$

where $R_m$ is the remainder. Similarly, we have

$$\begin{aligned}
\sum_{\partial(a)=m} f^2(a) &= \sum_{\partial(a)=m} \left( \sum_{p^k \| a} f(p^k) \right)^2 \\
&= \sum_{\partial(a)=m} \sum_{p^k \| a} f^2(p^k) + \sum_{\partial(a)=m} \sum_{\substack{p_1 \neq p_2 \\ p_1^k \| a,\, p_2^\ell \| a}} f(p_1^k) f(p_2^\ell) \\
&= S_1 + S_2, \qquad (1.8)
\end{aligned}$$

say. Then

$$\begin{aligned}
S_1 &= \sum_{k\partial(p) \leq m} f^2(p^k) \sum_{\substack{\partial(a)=m \\ p^k \| a}} 1 \\
&= Aq^m \Bigg[ \sum_{k\partial(p) \leq m} f^2(p^k) q^{-k\partial(p)} \left(1 - q^{-\partial(p)}\right) \\
&\quad + O\left( \sum_{k\partial(p) < m} |f^2(p^k)| q^{-k\partial(p)} (m - k\partial(p))^{-\gamma} \right) \Bigg] \\
&\quad + \sum_{k\partial(p)=m} f^2(p^k) \left(1 - A(1 - q^{-\partial(p)})\right). \qquad (1.9)
\end{aligned}$$

Also,

$$S_2 = \sum_{\substack{p_1 \neq p_2 \\ k\partial(p_1) \leq m,\, \ell\partial(p_2) \leq m}} f(p_1^k) f(p_2^\ell) \sum_{\substack{\partial(a)=m \\ p_1^k \| a,\, p_2^\ell \| a}} 1.$$

The inner sum on the right-hand side equals

$$Aq^{m-k\partial(p_1)-\ell\partial(p_2)} \left(1 - q^{-\partial(p_1)}\right) \left(1 - q^{-\partial(p_2)}\right) + O\left( \frac{q^{m-k\partial(p_1)-\ell\partial(p_2)}}{(m - k\partial(p_1) - \ell\partial(p_2))^\gamma} \right)$$

for $k\partial(p_1) + \ell\partial(p_2) < m$ (see Lemma 7.3.3). Hence

$$S_2 = Aq^m \Bigg[ \sum_{\substack{p_1 \neq p_2 \\ k\partial(p_1) + \ell\partial(p_2) \leq m}} f(p_1^k) f(p_2^\ell) q^{-k\partial(p_1)-\ell\partial(p_2)}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

$$
\begin{aligned}
&\times \left(1 - q^{-\partial(p_1)}\right)\left(1 - q^{-\partial(p_2)}\right) \\
&+O\Bigg( \sum_{\substack{p_1 \neq p_2 \\ k\partial(p_1)+\ell\partial(p_2)<m}} \left|f(p_1^k) f(p_2^\ell)\right| q^{-k\partial(p_1)-\ell\partial(p_2)} \\
&\qquad \times \left(m - k\partial(p_1) - \ell\partial(p_2)\right)^{-\gamma} \Bigg)\Bigg] \\
&+ \sum_{\substack{p_1 \neq p_2 \\ k\partial(p_1)+\ell\partial(p_2)=m}} f(p_1^k) f(p_2^\ell) \\
&\qquad \times \left[1 - A\left(1 - q^{-\partial(p_1)}\right)\left(1 - q^{-\partial(p_2)}\right)\right]. \qquad (1.10)
\end{aligned}
$$

From (1.8), (1.9), (1.10), and (1.7), we can write the variance

$$
\begin{aligned}
&\frac{1}{G(m)} \sum_{\partial(a)=m} f^2(a) - \frac{1}{G^2(m)} \left( \sum_{\partial(a)=m} f(a) \right)^2 \\
&= \sum_{k\partial(p)\leq m} f^2(p^k) q^{-k\partial(p)} + Q_m, \qquad (1.11)
\end{aligned}
$$

where $Q_m$ is the remainder.

## 7.2 Limit Distribution Functions of Real–Valued Additive Functions

We first prove the following analogue of the *Erdős–Wintner* theorem in classical probabilistic number theory (cf. Erdős and Wintner [1], Elliott [1]). The proof is based on Theorem 6.4.1 of Chapter 6, and Lemma 7.1.4, the continuity theorem.

(7.2.1) THEOREM. (cf. Zhang [3]) *Suppose (i) that $\mathcal{G}$ is a Chebyshev additive arithmetical semigroup, satisfying*

$$\sum_{n=1}^{\infty} \left|G(n)q^{-n} - A\right| < \infty$$

*with constants $A > 0$ and $q > 1$, or (ii) that*

$$\sum_{n=1}^{\infty} \sup_{n \leq m} \left|G(m)q^{-m} - A\right| < \infty$$

*holds. Then a real–valued additive function $f$ on $\mathcal{G}$ has a limit distribution function $F(x)$ if and only if the three series*

$$\sum_{|f(p)|\geq 1} q^{-\partial(p)}, \quad \sum_{|f(p)|<1} f(p)q^{-\partial(p)}, \quad \sum_{|f(p)|<1} f^2(p)q^{-\partial(p)} \tag{2.1}$$

*all converge. Moreover, the limit distribution function $F(x)$ has the characteristic function*

$$\phi(t) = \prod_{p} \left(1 - q^{-\partial(p)}\right) \left(1 + \sum_{k=1}^{\infty} q^{-k\partial(p)} e^{itf(p^k)}\right), \tag{2.2}$$

*where the infinite product is taken over all $p \in \mathcal{P}$ in ascending order of $\partial(p)$.*

*Remark.* Our proof of the sufficiency of the conditions follows the idea of Delange [1]. A direct proof is certainly possible also.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

PROOF. It is sufficient to prove the theorem under condition (i) since condition (ii) implies (i). By the continuity theorem, $f$ has a limit distribution function $F(x)$ if and only if there exists a function $\phi(t)$ which is continuous at $t = 0$ such that

$$\int_{-\infty}^{\infty} e^{itx} d\left(\frac{\nu_m(f,x)}{G(m)}\right) = \frac{1}{G(m)} \sum_{\partial(a)=m} e^{itf(a)} \to \phi(t) \tag{2.3}$$

as $m \to \infty$ for $-\infty < t < \infty$. Moreover, $\phi(t)$ is the characteristic function of $F(x)$. We note that the function $g(a) := e^{itf(a)}$ is multiplicative, and $|g(a)| = 1$ since $f(a)$ is real–valued and additive. Hence, by Theorem 6.4.1 of Chapter 6, (2.3) holds with $\phi(t)$ given in (2.2) if the series

$$\sum_p q^{-\partial(p)} \left(1 - e^{itf(p)}\right) \tag{2.4}$$

converges for $-\infty < t < \infty$. Actually, if

$$1 + \sum_{k=1}^{\infty} e^{itf(p^k)} q^{-k\partial(p)} \neq 0$$

for each $p$ with $\partial(p) \leq \frac{\log 2}{\log q}$, then (2.3) holds with $\phi(t)$ as given in (2.2), and if

$$1 + \sum_{k=1}^{\infty} e^{itf(p^k)} q^{-k\partial(p)} = 0$$

for some $p$ with $\partial(p) \leq \frac{\log 2}{\log q}$, then $\phi(t)$ given in (2.2) is zero and (2.3) holds again. Conversely, if (2.3) holds with $\phi(t) \neq 0$ for some $t$, then, by the same theorem, (2.4) converges and $\phi(t)$ is given by (2.2).

Now, suppose first that the three series in (2.1) are all convergent. We claim that this implies the uniform convergence of the series (2.4) for $|t| \leq T$ for each $T > 0$. This implies immediately that $f$ has a limit distribution function $F(x)$ which has the characteristic function $\phi(t)$ given in (2.2). Actually, we may write the series (2.4) as

$$\sum_p q^{-\partial(p)} \left(1 + itf(p) - e^{itf(p)}\right) h(p) - \sum_p q^{-\partial(p)} itf(p)h(p)$$
$$+ \sum_p q^{-\partial(p)} \left(1 - e^{itf(p)}\right)(1 - h(p)), \tag{2.5}$$

where

$$h(p) := \begin{cases} 1 & \text{for } |f(p)| < 1, \\ 0 & \text{for } |f(p)| \geq 1. \end{cases}$$

Applying the simple inequality

$$\left| e^{i\beta} - 1 - i\beta \right| \leq \min \left\{ \frac{\beta^2}{2}, 2|\beta| \right\},$$

which holds for each real number $\beta$, we have

$$\left| 1 + itf(p) - e^{itf(p)} \right| \leq \frac{1}{2} t^2 f^2(p),$$

and hence the first series in (2.5) converges absolutely and uniformly for $|t| \leq T$. Then it is plain that the second series in (2.5) converges uniformly for $|t| \leq T$. Finally, the last series in (2.5) converges absolutely and uniformly for $-\infty < t < \infty$. This proves the claim.

Suppose then that $f$ has a limit distribution function $F(x)$ with a characteristic function $\phi(t)$. There exists a constant $T > 0$ such that

$$|\phi(t)| > \frac{1}{2} \quad \text{for} \quad |t| \leq T,$$

since $\phi(t)$ is (uniformly) continuous, and $\phi(0) = 1$. Thus (2.3) holds for $|t| \leq T$, and $\phi(t)$ must be of the form (2.2). Moreover, the series (2.4) converges for $|t| \leq T$.

We need to show that the three series in (2.1) are convergent. To this end, write

$$\phi(t) = \phi_1(t)\phi_2(t)\phi_3(t),$$

where

$$\phi_1(t) := \prod_{\partial(p) < M} \left( 1 - q^{-\partial(p)} \right) \left( 1 + \sum_{k=1}^{\infty} q^{-k\partial(p)} e^{itf(p^k)} \right)$$

is a finite product of continuous functions,

$$\begin{aligned} \phi_2(t) :\ &= \prod_{\partial(p)\geq M} \left(1 - q^{-\partial(p)}\right)\left(1 - q^{-\partial(p)} e^{itf(p)}\right)^{-1} \\ &= \exp\left\{ - \sum_{\partial(p)\geq M} q^{-\partial(p)} \left(1 - e^{itf(p)}\right) \right. \\ &\qquad \left. + \sum_{\partial(p)\geq M} \sum_{k=2}^{\infty} \frac{1}{k} q^{-k\partial(p)} \left(-1 + e^{itkf(p)}\right) \right\}, \end{aligned} \tag{2.6}$$

and

$$\begin{aligned} \phi_3(t) :\ &= \prod_{\partial(p)\geq M} \left(1 - q^{-\partial(p)} e^{itf(p)}\right)\left(1 + \sum_{k=1}^{\infty} q^{-k\partial(p)} e^{itf\left(p^k\right)}\right) \\ &= \prod_{\partial(p)\geq M} \left(1 + \sum_{k=2}^{\infty} q^{-k\partial(p)} \left(e^{itf\left(p^k\right)} - e^{it\left(f\left(p^{k-1}\right)+f(p)\right)}\right)\right). \end{aligned} \tag{2.7}$$

Note that $\phi_1(t)$ is continuous and hence has an upper bound for $|t| \leq T$. Therefore

$$|\phi_2(t)\phi_3(t)| \gg 1 \quad \text{for} \quad |t| \leq T.$$

Then note that the infinite product on the right–hand side of (2.7) converges uniformly for $-\infty < t < \infty$, since each factor function (sum of an infinite series) is non–vanishing provided that $M$ is sufficiently large, and since

$$\begin{aligned} &\sum_{\partial(p)\geq M} \sum_{k=2}^{\infty} q^{-k\partial(p)} \left| e^{itf\left(p^k\right)} - e^{it\left(f\left(p^{k-1}\right)-f(p)\right)} \right| \\ &\leq\ 2 \sum_{\partial(p)\geq M} \sum_{k=2}^{\infty} q^{-k\partial(p)} \ll \sum_{m\geq M} P(m) q^{-2m} \\ &\ll\ \sum_{m\geq M} q^{-m} m^{-1} < \infty. \end{aligned}$$

Hence $\phi_3(t)$ is also continuous, and has an upper bound on $|t| \leq T$. Therefore

$$|\phi_2(t)| \gg 1 \quad \text{for} \quad |t| \leq T. \tag{2.8}$$

Finally note that the first series on the right–hand side of (2.6) is exactly the series (2.4) without regarding the first few terms, and that the second series on the right–hand side of (2.6) converges uniformly for $-\infty < t < \infty$. It follows, from (2.8), that

$$\left|\exp\left\{-\sum_{\partial(p)\geq M} q^{-\partial(p)}\left(1-e^{itf(p)}\right)\right\}\right| \gg 1$$

for $|t| \leq T$, and hence

$$Re\sum_{p} q^{-\partial(p)}\left(1-e^{itf(p)}\right) \leq K$$

(only a finite number of $p$ satisfying $\partial(p) \leq M$!), or, equivalently

$$\sum_{p} q^{-\partial(p)}\left(1-\cos\, tf(p)\right) = 2\sum_{p} q^{-\partial(p)}\sin^2\left(\frac{tf(p)}{2}\right) \leq K \qquad (2.9)$$

for $|t| \leq T$. This implies that

$$2\sum_{T|f(p)|\leq\frac{\pi}{2}} q^{-\partial(p)}\left(\frac{2}{\pi}\right)^2\frac{T^2f^2(p)}{2^2} \leq K,$$

and then

$$\sum_{|f(p)|\leq\delta} q^{-\partial(p)}f^2(p) \ll \frac{1}{T^2} \qquad (2.10)$$

with $\delta = \frac{\pi}{2T}$. Also, integrating (2.9) gives

$$\sum_{p} q^{-\partial(p)}\int_0^T \left(1-\cos\, tf(p)\right)dt \leq KT,$$

and we obtain

$$\sum_{T|f(p)|\geq\frac{\pi}{2}} q^{-\partial(p)}\left(T-\frac{|\sin\, Tf(p)|}{|f(p)|}\right) \leq KT,$$

and then

$$\sum_{|f(p)|\geq\delta} q^{-\partial(p)}T\left(1-\frac{2}{\pi}\right) \leq KT.$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

It follows that

$$\sum_{|f(p)|\geq\delta} q^{-\partial(p)} \ll 1. \tag{2.11}$$

Now, (2.10) and (2.11) imply the convergence of the first and the third series in (2.1).

To show the convergence of the second series in (2.1), note that the imaginary part of (2.4) is

$$-\sum_{p} q^{-\partial(p)} \sin\left(tf(p)\right),$$

which converges for $|t| \leq T$. This fact and the convergence of the first series in (2.1) imply that

$$\sum_{|f(p)|<1} q^{-\partial(p)} \sin\left(tf(p)\right)$$

converges for $|t| \leq T$. We note that

$$|\sin\left(tf(p)\right) - tf(p)| \leq \frac{|tf(p)|^3}{3!},$$

for $|t|$ sufficiently small and $|f(p)| < 1$, and, from the convergence of the third series in (2.1), that

$$\sum_{|f(p)|<1} q^{-\partial(p)} |tf(p)|^3$$

converges. It follows that

$$\sum_{|f(p)|<1} q^{-\partial(p)} tf(p)$$

converges, and then the second series in (2.1) does too. □

## 7.3 An Analogue of the Turán–Kubilius Inequality

In this section, we assume that

$$G(m) = Aq^m + O\left(q^m m^{-\gamma}\right), \quad m \geq 1 \tag{3.1}$$

holds with constants $A > 0$, $q > 1$, and $\gamma > 1$. We shall then establish an analogue of the classical *Turán–Kubilius inequality* (cf. Elliott [1]) in Lemma 7.3.1.

Let $f(a)$ be a complex-valued additive function on an arithmetical semigroup $\mathcal{G}$, so that

$$f(a) = \sum_{p^k \| a} f(p^k),$$

where as usual $p^k \| a$ signifies that $p^k$ is the highest power of $p$ dividing $a$. For $m > 0$, set

$$E(m) := \sum_{k\partial(p) \leq m} f(p^k) q^{-k\partial(p)} \left(1 - q^{-\partial(p)}\right),$$

and

$$D(m) := \left( \sum_{k\partial(p) \leq m} |f(p^k)|^2 q^{-k\partial(p)} \right)^{\frac{1}{2}} \geq 0$$

(see (1.7) and (1.11)).

(7.3.1) Lemma. (cf. Zhang [3]). *There exists a constant $K$ depending only on the constants $A$, $q$, $\gamma$, and the $O$-constant in (3.1), such that*

$$\sum_{\partial(a)=m} |f(a) - E(m)|^2 \leq KG(m)D^2(m). \tag{3.2}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Before giving a proof of Lemma 7.3.1, we record here the following interesting "dual" of the inequality (3.2), although it is not used subsequently in this chapter.

(7.3.2) LEMMA. *The inequality*

$$\sum_{k\partial(p)\le m} q^{k\partial(p)} \left| \sum_{\substack{\partial(a)=m \\ p^k \| a}} g(a) - q^{-k\partial(p)}\left(1-q^{-\partial(p)}\right) \sum_{\partial(a)=m} g(a) \right|^2$$

$$\le KG(m) \sum_{\partial(a)=m} |g(a)|^2 \tag{3.3}$$

*holds for any complex–valued function $g$ on $\mathcal{G}$.*

PROOF. Let

$$C(p^k,a) = \begin{cases} q^{k\partial(p)/2} - q^{-k\partial(p)/2}\left(1-q^{-\partial(p)}\right), & \text{if } p^k \| a, \\ -q^{-k\partial(p)/2}\left(1-q^{-\partial(p)}\right), & \text{otherwise.} \end{cases}$$

If we replace $f(p^k)$ by $f(p^k)q^{k\partial(p)/2}$ in (3.2), then the inequality obtained may be rewritten in the form

$$\sum_{\partial(a)=m} \left| \sum_{k\partial(p)\le m} f(p^k)C(p^k,a) \right|^2 \le KG(m) \sum_{k\partial(p)\le m} |f(p^k)|^2.$$

The inequality (3.3) follows by applying the "principle of duality" (Elliott [1], Chapter 4, Lemma 4.3) to the above inequality. □

In order to prove Lemma 3.1, we need several elementary estimates. We remark, once and for all, that all $O$–constants in these estimates depend only on the constants $A$, $q$, $\gamma$ and the $O$–constant in (3.1).

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

(7.3.3) LEMMA. *For any positive integer $m$, a non-negative integer $k$, and a prime $p \in \mathcal{G}$ such that $k\partial(p) < m$, we have*

$$\sum_{\substack{a \\ \partial(a)=m \\ p^k \| a}} 1 = Aq^{m-k\partial(p)}\left(1-q^{-\partial(p)}\right) + O\left(\frac{q^{m-k\partial(p)}}{(m-k\partial(p))^{\gamma}}\right). \tag{3.4}$$

*Also, for any positive integer $m$, non-negative integers $k$ and $\ell$, and distinct primes $p_1$ and $p_2$ such that $k\partial(p_1)+\ell\partial(p_2) < m$, we have*

$$\begin{aligned}\sum_{\substack{a \\ \partial(a)=m \\ p_1^k\|a,\, p_2^\ell\|a}} 1 \;=\; & Aq^{m-k\partial(p_1)-\ell\partial(p_2)}\left(1-q^{-\partial(p_1)}\right)\left(1-q^{-\partial(p_2)}\right) \\ & + O\left(\frac{q^{m-k\partial(p_1)-\ell\partial(p_2)}}{(m-k\partial(p_1)-\ell\partial(p_2))^{\gamma}}\right). \end{aligned}\tag{3.5}$$

PROOF. We may write $a = p_1^k p_2^\ell a'$ on the left–hand side of (3.5), with $(a', p_1p_2) = 1$ and $\partial(a') = m - k\partial(p_1) - \ell\partial(p_2)$. Hence

$$\begin{aligned}\sum_{\substack{a \\ \partial(a)=m \\ p_1^k\|a,\, p_2^\ell\|a}} 1 \;=\; & \sum_{\substack{a' \\ (a',p_1p_2)=1 \\ \partial(a')=m-k\partial(p_1)-\ell\partial(p_2)}} 1 \\ =\; & \sum_{\substack{a' \\ \partial(a')=m-k\partial(p_1)-\ell\partial(p_2)}} 1 - \sum_{\substack{a' \\ \partial(a')=m-(k+1)\partial(p_1)-\ell\partial(p_2)}} 1 \\ & - \sum_{\substack{a' \\ \partial(a')=m-k\partial(p_1)-(\ell+1)\partial(p_2)}} 1 + \sum_{\substack{a' \\ \partial(a')=m-(k+1)\partial(p_1)-(\ell+1)\partial(p_2)}} 1.\end{aligned}$$

Then (3.5) follows from (3.1) by calculation. For simplicity, we consider only the case that $(k+1)\partial(p_1)+\ell\partial(p_1) < m$ and $k\partial(p_1)+(\ell+1)\partial(p_2) \geq m$; a similar calculation applies to other cases. Thus we have

$$\begin{aligned}\sum_{\substack{a \\ \partial(a)=m \\ p_1^k\|a,\, p_2^\ell\|a}} 1 \;=\; & G\left(m-k\partial(p_1)-\ell\partial(p_2)\right) \\ & - G\left(m-(k+1)\partial(p_1)-\ell\partial(p_2)\right) + r,\end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

where $r = 1$ or $0$ according as $k\partial(p_1) + (\ell + 1)\partial(p_2) = m$ or not. By (3.1), the right–hand side equals

$$Aq^{m-k\partial(p_1)-\ell\partial(p_2)}\left(1 - q^{-\partial(p_1)}\right) + O\left(\frac{q^{m-k\partial(p_1)-\ell\partial(p_2)}}{(m - k\partial(p_1) - \ell\partial(p_2))^\gamma}\right).$$

Note that $\partial(p_1) < m - k\partial(p_1) - \ell\partial(p_2) \le \partial(p_2)$, and hence $(m - k\partial(p_1) - \ell\partial(p_2))^\gamma \le (\partial(p_2))^\gamma \ll q^{\partial(p_2)}$, since $q > 1$. Therefore

$$\begin{aligned}\sum_{\substack{a \\ \partial(a)=m \\ p_1^k \| a,\, p_2^\ell \| a}} 1 &= Aq^{m-k\partial(p_1)-\ell\partial(p_2)}\left(1 - q^{-\partial(p_1)}\right)\left(1 - q^{-\partial(p_2)}\right) \\ &\quad + O\left(\frac{q^{m-k\partial(p_1)-\ell\partial(p_2)}}{(m - k\partial(p_1) - \ell\partial(p_2))^\gamma}\right).\end{aligned}$$

This proves (3.5) in this case.

Similarly, we can prove (3.4). □

(7.3.4) Lemma. *For any complex–valued function $f$,*

$$E(m) \ll D(m)(\log m)^{\frac{1}{2}}. \tag{3.6}$$

Proof. By the Cauchy–Schwarz inequality,

$$|E(m)| \le \left[\sum_{k\partial(p)\le m} \left|f(p^k)\right|^2 q^{-k\partial(p)}\right]^{\frac{1}{2}} \left[\sum_{k\partial(p)\le m} q^{-k\partial(p)}\right]^{\frac{1}{2}}.$$

The sum in the second factor on the right–hand side equals

$$\begin{aligned}\sum_{1\le n\le m} q^{-m} \sum_{\substack{p,k \\ k\partial(p)=n}} 1 &= \sum_{1\le n\le m} q^{-n} \sum_{k|n} P\left(\frac{n}{k}\right) \\ &= \sum_{1\le n\le m} q^{-n} O\left(q^n n^{-1}\right) = O(\log m),\end{aligned}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

by (3.11) of Chapter 3. □

(7.3.5) LEMMA. *For any non–negative function $f$,*

$$\sum_{\partial(a)=m} f^2(a) \le Aq^m E^2(m) + O\left(q^m D^2(m)\right). \tag{3.7}$$

*Also, for any complex–valued function $f$,*

$$\sum_{\partial(a)=m} f(a) = Aq^m E(m) + O\left(q^m D(m) m^{-\frac{1}{2}}\right). \tag{3.8}$$

PROOF. To prove (3.7), write

$$\begin{aligned} S_1 : &= \sum_{\partial(a)=m} f^2(a) = \sum_{\partial(a)=m} \left( \sum_{\substack{p \\ p^k || a}} f(p^k) \right)^2 \\ &= \sum_{\partial(a)=m} \left[ \sum_{\substack{p \\ p^k || a}} f^2(p^k) + \sum_{\substack{p_1 \neq p_2 \\ p_1^k || a, p_2^\ell || a}} f(p_1^k) f(p_2^\ell) \right] \\ &= \sum_{k\partial(p)=m} f^2(p^k) \sum_{\substack{a \\ \partial(a)=m \\ p^k || a}} 1 + \sum_{\substack{p_1 \neq p_2 \\ k\partial(p_1)+\ell\partial(p_2) \le m}} f(p_1^k) f(p_2^\ell) \sum_{\substack{a \\ \partial(a)=m \\ p_1^k || a, p_2^\ell || a}} 1 \\ &= S_2 + S_3, \end{aligned} \tag{3.9}$$

say. By (3.4),

$$\begin{aligned} S_2 &= \sum_{k\partial(p)<m} f^2(p^k) \left[ Aq^{m-k\partial(p)} \left(1 - q^{-\partial(p)}\right) + O\left( \frac{q^{m-k\partial(p)}}{(m - k\partial(p))^\gamma} \right) \right] \\ &\quad + \sum_{k\partial(p)=m} f^2(p^k) \\ &\ll q^m D^2(m). \end{aligned} \tag{3.10}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

By (3.5),

$$\begin{aligned}
S_3 &= \sum_{\substack{p_1\neq p_2\\ k\partial(p_1)+\ell\partial(p_2)<m}} f(p_1^k)f(p_2^\ell)\Bigg[Aq^{m-k\partial(p_1)-\ell\partial(p_2)}\\
&\qquad \times\left(1-q^{-\partial(p_1)}\right)\left(1-q^{-\partial(p_2)}\right)+O\left(\frac{q^{m-k\partial(p_1)-\ell\partial(p_2)}}{(m-k\partial(p_1)-\ell\partial(p_2))^{\gamma}}\right)\Bigg]\\
&\quad+\sum_{\substack{p_1\neq p_2\\ k\partial(p_1)+\ell\partial(p_2)=m}} f(p_1^k)f(p_2^\ell)\\
&= Aq^m \sum_{\substack{p_1\neq p_2\\ k\partial(p_1)+\ell\partial(p_2)\leq m}} f(p_1^k)f(p_2^\ell)q^{-k\partial(p_1)-\ell\partial(p_2)}\\
&\qquad \times\left(1-q^{-\partial(p_1)}\right)\left(1-q^{-\partial(p_2)}\right)\\
&\quad+O\left(q^m \sum_{\substack{p_1\neq p_2\\ k\partial(p_1)+\ell\partial(p_2)<m}} f(p_1^k)f(p_2^\ell)\frac{q^{-k\partial(p_1)-\ell\partial(p_2)}}{(m-k\partial(p_1)-\ell\partial(p_2))^{\gamma}}\right)\\
&\quad+\sum_{\substack{p_1\neq p_2\\ k\partial(p_1)+\ell\partial(p_2)=m}} f(p_1^k)f(p_2^\ell)\left[1-A\left(1-q^{-\partial(p_1)}\right)\left(1-q^{-\partial(p_2)}\right)\right]\\
&= S_4+O(S_5)+S_6, \qquad (3.11)
\end{aligned}$$

say. Since $f$ is non–negative,

$$\begin{aligned}
S_4 &\leq Aq^m\left[\sum_{k\partial(p)\leq m} f(p^k)q^{-k\partial(p)}\left(1-q^{-\partial(p)}\right)\right]^2\\
&= Aq^mE^2(m). \qquad (3.12)
\end{aligned}$$

Then, by the Cauchy–Schwarz inequality,

$$S_5 \leq q^m\left[\sum_{\substack{p_1\neq p_2\\ k\partial(p_1)+\ell\partial(p_2)<m}}\left(f^2(p_1^k)q^{-k\partial(p_1)}\right)\left(f^2(p_2^\ell)q^{-\ell\partial(p_2)}\right)\right]^{\frac{1}{2}}$$

$$\times \left[ \sum_{\substack{p_1\neq p_2\\ k\partial(p_1)+\ell\partial(p_2)<m}} \frac{q^{-k\partial(p_1)-\ell\partial(p_2)}}{(m-k\partial(p_1)-\ell\partial(p_2))^{2\gamma}} \right]^{\frac{1}{2}}$$
$$\ll q^m D^2(m), \tag{3.13}$$

since

$$\sum_{\substack{p_1\neq p_2\\ k\partial(p_1)+\ell\partial(p_2)<m}} \frac{q^{-k\partial(p_1)-\ell\partial(p_2)}}{(m-k\partial(p_1)-\ell\partial(p_2))^{2\gamma}} = \sum_{n=1}^{m-1} \frac{q^{-n}}{(m-n)^{2\gamma}} \sum_{\substack{p_1\neq p_2\\ k\partial(p_1)+\ell\partial(p_2)=n}} 1$$
$$\leq \sum_{n=1}^{m-1} \frac{q^{-n}}{(m-n)^{2\gamma}} G(n) = \sum_{n=1}^{m-1} \frac{A}{(m-n)^{2\gamma}} + O\left( \sum_{n=1}^{m-1} \frac{1}{(m-n)^{2\gamma} n^{\gamma}} \right)$$
$$= O(1)$$

for $\gamma > 1$. Finally, by the Cauchy–Schwarz inequality again,

$$S_6 \ll \sum_{\substack{p_1\neq p_2\\ k\partial(p_1)+\ell\partial(p_2)=m}} f(p_1^k) f(p_2^\ell)$$
$$\leq \left[ \sum_{\substack{p_1\neq p_2\\ k\partial(p_1)+\ell\partial(p_2)=m}} \left(f^2(p_1^k) q^{-k\partial(p_1)}\right) \left(f^2(p_2^\ell) q^{-\ell\partial(p_2)}\right) \right]^{\frac{1}{2}}$$
$$\times \left[ \sum_{\substack{p_1\neq p_2\\ k\partial(p_1)+\ell\partial(p_2)=m}} q^{k\partial(p_1)+\ell\partial(p_2)} \right]^{\frac{1}{2}}$$
$$q^m D^2(m), \tag{3.14}$$

since

$$\sum_{\substack{p_1\neq p_2\\ k\partial(p_1)+\ell\partial(p_2)=m}} q^{k\partial(p_1)+\ell\partial(p_2)} = q^m \sum_{\substack{p_1\neq p_2\\ k\partial(p_1)+\ell\partial(p_2)=m}} 1 \leq q^m G(m) \ll q^{2m}.$$

From (3.9), (3.10), (3.11), (3.12), (3.13), and (3.14), (3.7) follows.

We now prove (3.8). Let

$$S_7 := \sum_{\partial(a)=m} f(a) = \sum_{\partial(a)=m} \sum_{\substack{p \\ p^k \| a}} f(p^k) = \sum_{k\partial(p)\leq m} f(p^k) \sum_{\substack{a \\ \partial(a)=m \\ p^k \| a}} 1.$$

By (3.4),

$$\begin{aligned} S_7 &= \sum_{k\partial(p)<m} f(p^k)\left[Aq^{m-k\partial(p)}\left(1-q^{-\partial(p)}\right)+O\left(\frac{q^{m-k\partial(p)}}{(m-k\partial(p))^{\gamma}}\right)\right] \\ &\quad + \sum_{k\partial(p)=m} f(p^k) \\ &= Aq^m \sum_{k\partial(p)\leq m} f(p^k)q^{-k\partial(p)}\left(1-q^{-\partial(p)}\right) \\ &\quad + \sum_{k\partial(p)=m} f(p^k)\left(1-A\left(1-q^{-\partial(p)}\right)\right) \\ &\quad +O\left(q^m \sum_{k\partial(p)<m} \left|f(p^k)\right| \frac{q^{-k\partial(p)}}{(m-k\partial(p))^{\gamma}}\right). \end{aligned} \tag{3.15}$$

By the Cauchy–Schwarz inequality and (3.11) of Chapter 3, the second term on the right-hand side of (3.15) is

$$\begin{aligned} &\ll \sum_{k\partial(p)=m} \left|f(p^k)\right| \leq \left(\sum_{k\partial(p)=m} \left|f(p^k)\right|^2 q^{-k\partial(p)}\right)^{\frac{1}{2}} \left(\sum_{k\partial(p)=m} q^{k\partial(p)}\right)^{\frac{1}{2}} \\ &\leq D(m)\left(q^m \sum_{n|m} P(n)\right)^{\frac{1}{2}} \ll q^m D(m) m^{-\frac{1}{2}}. \end{aligned} \tag{3.16}$$

Finally, by the Cauchy–Schwarz inequality again,

$$\begin{aligned} &\sum_{k\partial(p)<m} \left|f(p^k)\right| \frac{q^{-k\partial(p)}}{(m-k\partial(p))^{\gamma}} \\ &\leq \left[\sum_{k\partial(p)<m} \left|f(p^k)\right|^2 q^{-k\partial(p)}\right]^{\frac{1}{2}} \left[\sum_{k\partial(p)<m} \frac{q^{-k\partial(p)}}{(m-k\partial(p))^{2\gamma}}\right]^{\frac{1}{2}} \\ &\ll D(m)m^{-\frac{1}{2}} \end{aligned} \tag{3.17}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

since, by (3.11) of Chapter 3,

$$\begin{aligned}
\sum_{k\partial(p)<m} \frac{q^{-k\partial(p)}}{(m-k\partial(p))^{2\gamma}} &= \sum_{n=1}^{m-1} \frac{q^{-n}}{(m-n)^{2\gamma}} \sum_{k\partial(p)=n} 1 \\
&= \sum_{n=1}^{m-1} \frac{q^{-n}}{(m-n)^{2\gamma}} \sum_{\ell\mid n} P(\ell) \ll \sum_{n=1}^{m-1} \frac{1}{n(m-n)^{2\gamma}} \\
&= \left( \sum_{1\leq n\leq \frac{m}{2}} + \sum_{\frac{m}{2}<n\leq m-1} \right) \frac{1}{n(m-n)^{2\gamma}} \\
&\ll m^{-2\gamma}\log m + m^{-1} \ll m^{-1}.
\end{aligned}$$

Thus (3.8) follows from (3.15), (3.16), and (3.17). □

Proof of Lemma 3.1 We first assume that $f$ is real–valued and non–negative. By (3.7), (3.8), and (3.6), we have

$$\begin{aligned}
\sum_{\partial(a)=m} |f(a)-E(m)|^2 &= \sum_{\partial(a)=m} f^2(a) - 2E(m) \sum_{\partial(a)=m} f(a) + G(m)E^2(m) \\
&\leq Aq^m E^2(m) + O\left(q^m D^2(m)\right) \\
&\quad -2E(m)\left(Aq^m E(m) + O\left(q^m D(m) m^{-\frac{1}{2}}\right)\right) + G(m)E^2(m) \\
&= E^2(m) O\left(q^m m^{-\gamma}\right) + O\left(q^m D^2(m)\right) + O\left(q^m |E(m)| D(m) m^{-\frac{1}{2}}\right) \\
&= O\left(q^m D^2(m)\left[m^{-\gamma}\log m + 1 + m^{-\frac{1}{2}}(\log m)^{\frac{1}{2}}\right]\right),
\end{aligned}$$

and (3.2) follows.

Then assume that $f$ is real–valued. Define additive functions $f_1$ and $f_2$ by

$$f_1(p^k) = \frac{\left|f(p^k)\right| + f(p^k)}{2}, \quad f_2(p^k) = \frac{\left|f(p^k)\right| - f(p^k)}{2},$$

and, accordingly,

$$E_j(m) = \sum_{k\partial(p)\leq m} f_j(p^k) q^{-k\partial(p)} \left(1 - q^{-\partial(p)}\right), \quad j = 1, 2.$$

Then, $f = f_1 - f_2$, $E(m) = E_1(m) - E_2(m)$, and

$$|f(a) - E(m)|^2 \leq 2|f_1(a) - E_1(m)|^2 + 2|f_2(a) - E_2(m)|^2.$$

It follows that

$$\begin{aligned}\sum_{\partial(a)=m} |f(a) - E(m)|^2 &\ll \sum_{\partial(a)=m} |f_1(a) - E_1(m)|^2 + \sum_{\partial(a)=m} |f_2(a) - E_2(m)|^2 \\ &\ll q^m \left( \sum_{k\partial(p)\leq m} f_1^2(p^k) q^{-k\partial(p)} + \sum_{k\partial(p)\leq m} f_2^2(p^k) q^{-k\partial(p)} \right) \\ &= q^m \sum_{k\partial(p)\leq m} f^2(p^k) q^{-k\partial(p)},\end{aligned}$$

i.e., (3.2) holds.

Finally, if $f$ is complex–valued, define

$$g_1(a) = Re\, f(a), \quad g_2(a) = Im\, f(a).$$

In a similar manner, we can deduce (3.2). □

We shall use the following variant of Lemma 7.3.1 in the proof of Theorem 7.6.1.

(7.3.6) LEMMA. *Let $f$ be a complex–valued strongly additive function on $\mathcal{G}$, and let*

$$\nu(m) := \sum_{\partial(p)\leq m} f(p) q^{-\partial(p)} \tag{3.18}$$

*and*

$$\sigma(m) := \left( \sum_{\partial(p)\leq m} |f(p)|^2 q^{-\partial(p)} \right)^{\frac{1}{2}}. \tag{3.19}$$

*Then*

$$\sum_{\partial(a)=m} |f(a) - \nu(m)|^2 \ll q^m \sigma^2(m). \tag{3.20}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

PROOF. The left-hand side of (3.20) equals

$$\begin{aligned}
&\sum_{\partial(a)=m} |(f(a)-E(m))+(E(m)-\nu(m))|^2 \\
&\quad= \sum_{\partial(a)=m} |f(a)-E(m)|^2 + 2Re(E(m)-\nu(m)) \sum_{\partial(a)=m} (\bar{f}(a)-\bar{E}(m)) \\
&\qquad +G(m)|E(m)-\nu(m)|^2, \qquad (3.21)
\end{aligned}$$

where $\bar{f}(a)$ and $\bar{E}(m)$ denote the complex conjugates of $f(a)$ and $E(m)$, respectively. Since a strongly additive function is additive, by Lemma 7.3.1, the first term on the right-hand side of (3.21) is $O\left(q^m D^2(m)\right)$. By (3.8), (3.1), and (3.6), the second term on the right-hand side of (3.21) is

$$O\left(|E(m)-\nu(m)|q^m D(m) m^{-\frac{1}{2}}\right).$$

Therefore it is sufficient to show that

$$|E(m)-\nu(m)| \ll \sigma(m), \qquad (3.22)$$

and

$$D^2(m) = O\left(\sigma^2(m)\right). \qquad (3.23)$$

Actually, we have

$$\begin{aligned}
|E(m)-\nu(m)| \;\le\; &\left| \sum_{\substack{k\partial(p)\le m \\ k\ge 2}} f(p) q^{-k\partial(p)} \left(1-q^{-\partial(p)}\right) \right| \\
&+ \left| \sum_{\partial(p)\le m} f(p) q^{-2\partial(p)} \right|. \qquad (3.24)
\end{aligned}$$

The first term on the right-hand side of (3.24) equals

$$\left| \sum_{\partial(p)\le m} f(p) q^{-\partial(p)/2} \left(1-q^{-\partial(p)}\right) \sum_{2\le k\le \frac{m}{\partial(p)}} q^{-\left(k-\frac{1}{2}\right)\partial(p)} \right|$$

$$\begin{aligned}
&\leq \left[\sum_{\partial(p)\leq m} |f(p)|^2 q^{-\partial(p)}\right]^{\frac{1}{2}} \\
&\qquad \times \left[\sum_{\partial(p)\leq m} \left(1-q^{-\partial(p)}\right)^2 \left(\sum_{2\leq k\leq \frac{m}{\partial(p)}} q^{-\left(k-\frac{1}{2}\right)\partial(p)}\right)^2\right]^{\frac{1}{2}} \\
&\leq \sigma(m)\left(\sum_{\partial(p)\leq m} q^{-3\partial(p)}\right)^{\frac{1}{2}} \ll \sigma(m),
\end{aligned}$$

by the Cauchy–Schwarz inequality, since

$$\begin{aligned}
\sum_{\partial(p)\leq m} q^{-3\partial(p)} &= \sum_{1\leq n\leq m} q^{-3n}P(n) \ll \sum_{1\leq n\leq m} q^{-2n}n^{-1} \\
&= O(1).
\end{aligned}$$

Similarly, the second term on the right-hand side of (3.24) is

$$\leq \left[\sum_{\partial(p)\leq m} |f(p)|^2 q^{-\partial(p)}\right]^{\frac{1}{2}} \left[\sum_{\partial(p)\leq m} q^{-3\partial(p)}\right]^{\frac{1}{2}} \ll \sigma(m).$$

Thus, (3.22) follows.

Finally, we have

$$\begin{aligned}
D^2(m)-\sigma^2(m) &= \sum_{\substack{k\partial(p)\leq m\\ k\geq 2}} |f(p)|^2 q^{-k\partial(p)} \\
&= \sum_{\partial(p)\leq m} |f(p)|^2 q^{-\partial(p)} \sum_{2\leq k\leq \frac{m}{\partial(p)}} q^{-(k-1)\partial(p)} \ll \sigma^2(m).
\end{aligned}$$

This proves (3.23). □

## 7.4 A Fundamental Lemma

In this section, we shall establish a pair of inequalities, which is the counterpart of a so-called *fundamental lemma* in classical probabilistic number theory (cf. Kubilius [1]), and in the theory of *sieve methods* (cf. Halberstam and Richert [1]).

Accordingly, this pair of inequalities is also called a "fundamental lemma" here. It will be used to analyze a probability model in the next section. Here we shall set up this lemma via a sifting process, as in the classical theory of sieve methods.

We first need an order relation in an arithmetical semigroup $\mathcal{G}$. Since each $G(m)$ is a finite number, elements $a$ of $\mathcal{G}$ can be arranged in a sequence for which $\partial(a)$ is monotonically increasing. This sequence defines an order relation on $\mathcal{G}$ in a natural way, denoted as usual by $<$, so that $a < a'$ implies $\partial(a) \leq \partial(a')$. Of course, many *different* order relations with this property may be defined in general. However the specific order relation chosen is not important for our purpose, because the fundamental lemma depends only on the degree mapping $\partial$ and is independent of the concrete order relation $<$, as we shall see.

Let $a$ be *squarefree* and $a \neq 1$, so that we can write the canonical prime decomposition of $a$ in the form

$$a = p_1 \cdots p_m \quad with \quad p_1 > \cdots > p_m.$$

As usual, let $\omega(a) = m$ denote the total number of distinct prime divisors of $a$. For convenience we introduce notations $\Delta(a) = p_1$ and $\delta(a) = p_m$, for the "largest" and the "least" prime divisors of $a$, respectively. Also, for completeness, put $\Delta(1) = 1$ and $\delta(1) = \infty > a$, for all $a \in \mathcal{G}$.

Let $\mathcal{P}^*$ be a set of primes of $\mathcal{G}$, $a \in \mathcal{G}$, and $r$ be a real number with

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

$r > 1$. We write

$$P^*(a) := \prod_{\substack{p<a \\ p\in\mathcal{P}^*}} p, \quad P_r^* := \prod_{\substack{\partial(p)\leq r \\ p\in\mathcal{P}^*}} p. \tag{4.1}$$

(Notice the slight difference between these two definitions.) Let $\chi$ be a function defined on $\mathcal{G}$ such that $\chi(1) = 1$, and define $\bar{\chi}(d)$ by

(i) $\bar{\chi}(1) = 0$

(ii) $\bar{\chi}(d) = \chi(d/\delta(d)) - \chi(d)$ for $d \neq 1$.

Then, for squarefree $a$,

$$\sum_{\substack{d|a \\ \Delta(a/d)<\delta(d)}} \bar{\chi}(d) = 1 - \chi(a).$$

This leads to the following identity which is an analogue of the *Fundamental Sieve Identity* treated by Halberstam and Richert [2].

(7.4.1) LEMMA. *For any complex-valued function $h$ on $\mathcal{G}$, and any element $w$ of $\mathcal{G}$ with $w > 1$, we have*

$$\begin{aligned}\sum_{d|P^*(w)} \mu(d)h(d) \quad &= \sum_{d|P^*(w)} \mu(d)\chi(d)h(d) \\ &\quad + \sum_{d|P^*(w)} \mu(d)\bar{\chi}(d) \sum_{t|P^*(\delta(d))} \mu(t)h(dt), \qquad (4.2)\end{aligned}$$

*where $\mu$ is the Möbius function on $\mathcal{G}$.*

PROOF. We have

$$\sum_{d|P^*(w)} \mu(d)h(d) - \sum_{d|P^*(w)} \mu(d)\chi(d)h(d)$$

$$= \sum_{d|P^*(w)} \mu(d)h(d) \sum_{\substack{t|d \\ \Delta(d/t)<\delta(t)}} \bar{\chi}(t)$$

$$= \sum_{t|P^*(w)} \bar{\chi}(t) \sum_{\substack{d|P^*(w) \\ t|d,\, \Delta(d/t)<\delta(t)}} \mu(d)h(d).$$

Let $d = td'$. Then the inner sum on the right-hand side equals

$$\mu(t) \sum_{\substack{d'|(P^*(w)/t) \\ \Delta(d')<\delta(t)}} \mu(d')h(d't) = \mu(t) \sum_{d'|P^*\left(\delta(t)\right)} \mu(d')h(d't). \qquad \square$$

Let $\mathcal{A}$ be a finite sequence of elements of $\mathcal{G}$, not necessarily distinct, and $\mathcal{A}_d$ denote the subsequence of $\mathcal{A}$ consisting of the elements divisible by $d$. We denote the cardinality of $\mathcal{A}$, or $\mathcal{A}_d$, by $|\mathcal{A}|$, or $|\mathcal{A}_d|$, and consider two "sifting" functions

$$S(\mathcal{A}, \mathcal{P}^*, w) = |\{a : \ a \in \mathcal{A}, \ (a, P^*(w)) = 1\}| \tag{4.3}$$

and

$$S(\mathcal{A}, \mathcal{P}^*, r) = |\{a : \ a \in \mathcal{A}, \ (a, P_r^*) = 1\}|, \tag{4.4}$$

where $(a, b) = 1$ indicates that $a$ and $b$ are coprime. Then, from Lemma 7.4.1, with $h(d) = |\mathcal{A}_d|$, we have

$$S(\mathcal{A}, \mathcal{P}^*, r) = \sum_{d|P_r^*} \mu(d)\chi(d)|\mathcal{A}_d| + \sum_{d|P_r^*} \mu(d)\bar{\chi}(d)S(\mathcal{A}_d, \mathcal{P}^*, \delta(d)). \tag{4.5}$$

(7.4.2) LEMMA. *Suppose that there exists a positive integer $n$ such that, for each divisor $d$ of $P_r^*$,*

$$|\mathcal{A}_d| = \begin{cases} Aq^{n-\partial(d)} + R_d, & \textit{if } \partial(d) < n, \\ R_d, & \textit{if } \partial(d) = n, \\ 0, & \textit{if } \partial(d) > n. \end{cases} \tag{4.6}$$

*If $\chi^+(d)$ is a function defined on divisors $d$ of $P_r^*$ such that $\bar{\chi}^+(d)$ is non-negative, and such that $\bar{\chi}^+(d) = 0$ when $\omega(d)$ is even, then*

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}^*, r) \; &\leq \; Aq^n \left( \prod_{p \mid P_r^*} \left(1 - q^{-\partial(p)}\right) \right) (1 - S^+) \qquad (4.7) \\ &\quad -Aq^n \sum_{\substack{d \mid P_r^* \\ \partial(d) \geq n}} \mu(d) \chi^+(d) q^{-\partial(d)} + \sum_{\substack{d \mid P_r^* \\ \partial(d) \leq n}} \mu(d) \chi^+(d) R_d, \end{aligned}$$

*where*

$$S^+ = \sum_{d \mid P_r^*} \mu(d) \bar{\chi}^+(d) q^{-\partial(d)} \prod_{\substack{p \mid P_r^* \\ \delta(d) \leq p}} \left(1 - q^{-\partial(d)}\right)^{-1}. \qquad (4.8)$$

*If $\chi^-(d)$ is a function defined on divisors $d$ of $P_r^*$ such that $\bar{\chi}^-(d)$ is non-negative, and such that $\bar{\chi}^-(d) = 0$ when $\omega(d)$ is odd, then*

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}^*, r) \; &\geq \; Aq^n \left( \prod_{p \mid P_r^*} \left(1 - q^{-\partial(p)}\right) \right) (1 - S^-) \qquad (4.9) \\ &\quad -Aq^n \sum_{\substack{d \mid P_r^* \\ \partial(d) \geq n}} \mu(d) \chi^-(d) q^{-\partial(d)} + \sum_{\substack{d \mid P_r^* \\ \partial(d) \leq n}} \mu(d) \chi^-(d) R_d, \end{aligned}$$

*where*

$$S^- = \sum_{d \mid P_r^*} \mu(d) \bar{\chi}^-(d) q^{-\partial(d)} \prod_{\substack{p \mid P_r^* \\ \delta(d) \leq p}} \left(1 - q^{-\partial(p)}\right)^{-1}. \qquad (4.10)$$

PROOF. For $d \nmid P_r^*$, let $\chi^{\pm}(d) = 0$. From (4.5), we have

$$S(\mathcal{A}, \mathcal{P}^*, r) \leq \sum_{d \mid P_r^*} \mu(d) \chi^+(d) |\mathcal{A}_d|. \qquad (4.11)$$

By (4.6), the sum on the right–hand side equals

$$\begin{aligned} &\sum_{\substack{d \mid P_r^* \\ \partial(d) < n}} \mu(d) \chi^+(d) \left(Aq^{n-\partial(d)} + R_d\right) + \sum_{\substack{d \mid P_r^* \\ \partial(d) = n}} \mu(d) \chi^+(d) R_d \\ &= S_1 + \sum_{\substack{d \mid P_r^* \\ \partial(d) \leq n}} \mu(d) \chi^+(d) R_d, \qquad (4.12) \end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

where

$$\begin{aligned} S_1 &= Aq^n \sum_{\substack{d \mid P_r^* \\ \partial(d)<n}} \mu(d)\chi^+(d)q^{-\partial(d)} \\ &= Aq^n \Bigg[ \sum_{d \mid P_r^*} \mu(d)q^{-\partial(d)} - \sum_{d \mid P_r^*} \mu(d)\bar{\chi}^+(d)q^{-\partial(d)} \sum_{t \mid P^*(\delta(d))} \mu(t)q^{-\partial(t)} \\ &\quad - \sum_{\substack{d \mid P_r^* \\ \partial(d)\geq n}} \mu(d)\chi^+(d)q^{-\partial(d)} \Bigg], \end{aligned} \tag{4.13}$$

by (4.2). The sum of the first two terms on the right-hand side of (4.13) can be written as

$$\begin{aligned} &\prod_{p \mid P_r^*} \left(1 - q^{-\partial(p)}\right) - \sum_{d \mid P_r^*} \mu(d)\bar{\chi}^+(d)q^{-\partial(d)} \prod_{p \mid P^*(\delta(d))} \left(1 - q^{-\partial(p)}\right) \\ &= \left( \prod_{p \mid P_r^*} \left(1 - q^{-\partial(p)}\right) \right) (1 - S^+), \end{aligned}$$

with $S^+$ defined in (4.8). This proves (4.7)

Similarly, we can prove (4.9). □

In order to arrive at the "fundamental lemma", we give $\chi^+(d)$ and $\chi^-(d)$ the *Buchstab–Rosser type* structure (cf. Iwaniec [1], Halberstam and Richert [1]) with two parameters $\beta$ and $Y$: Thus, for

$$d = p_1 p_2 \cdots p_k \quad \text{with} \quad p_1 > p_2 > \cdots > p_k,$$

we let

$$\chi^+(d) = \eta^+(p_1)\eta^+(p_1 p_2) \cdots \eta^+(p_1 p_2 \cdots p_k), \tag{4.14}$$

where

$$\eta^+(a) = \begin{cases} 1, & \text{if } \omega(a) \text{ is even,} \\ 1, & \text{if } \omega(a) \text{ is odd and } \beta\partial(\delta(a)) + \partial(a) < Y, \\ 0, & \text{otherwise,} \end{cases} \tag{4.15}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

and let

$$\chi^-(d) = \eta^-(p_1)\eta^-(p_1p_2)\cdots\eta^-(p_1p_2\cdots p_k), \tag{4.16}$$

where

$$\eta^-(a) = \begin{cases} 1, & \text{if } \omega(a) \text{ is odd,} \\ 1, & \text{if } \omega(a) \text{ is even and } \beta\partial(\delta(a)) + \partial(a) < Y, \\ 0, & \text{otherwise.} \end{cases} \tag{4.17}$$

Then, from (4.14),

$$\bar{\chi}^+(d) = \eta^+(p_1)\cdots\eta^+(p_1p_2\cdots p_{k-1})\left(1 - \eta^+(p_1p_2\cdots p_k)\right) \tag{4.18}$$

is non–negative, and $\bar{\chi}^+(d) = 0$ when $\omega(d) = k$ is even. Similarly,

$$\bar{\chi}^-(d) = \eta^-(p_1)\cdots\eta^-(p_1p_2\cdots p_{k-1})\left(1 - \eta^-(p_1p_2\cdots p_k)\right)$$

is non–negative, and $\bar{\chi}^-(d) = 0$ when $\omega(d) = k$ is odd. Thus (4.7) and (4.9) hold.

(7.4.3) LEMMA. *Let $\beta > 1$ and $Y \geq 2$. We have*

$$\frac{Y - \partial(\Delta(d))}{\partial(\delta(d))} \leq \beta\left(\frac{\beta+1}{\beta-1}\right)^{(\omega(d)-1)/2} \quad \text{if} \quad \bar{\chi}^+(d) = 1, \tag{4.19}$$

*and*

$$\frac{Y - \partial(\Delta(d))}{\partial(\delta(d))} \leq (\beta - 1)\left(\frac{\beta+1}{\beta-1}\right)^{\omega(d)/2} \quad \text{if} \quad \bar{\chi}^-(d) = 1. \tag{4.20}$$

PROOF. To prove (4.19), note that $\bar{\chi}^+(d) = 1$ implies that $\omega(d)$ is odd. Let

$$d = p_1p_2\cdots p_{2k+1} \quad \text{with} \quad p_1 > p_2 > \cdots > p_{2k+1}.$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Then

$$\chi^+(d) = \chi^+(p_1 \cdots p_{2k}) - \chi^+(p_1 \cdots p_{2k+1}) = 1,$$

and thus

$$\chi^+(p_1 p_2 \cdots p_{2k}) = 1, \quad \chi^+(p_1 p_2 \cdots p_{2k+1}) = 0.$$

By (4.14) and (4.15), this implies

$$(\beta + 1)\partial(p_1) < Y, \tag*{$(4.21)_1$}$$
$$(\beta + 1)\partial(p_3) + \partial(p_2) + \partial(p_1) < Y, \tag*{$(4.21)_2$}$$
$$\cdots\cdots \tag*{$\cdots\cdot$}$$
$$(\beta + 1)\partial(p_{2\ell-1}) + \partial(p_{2\ell-2}) + \cdots + \partial(p_1) < Y, \tag*{$(4.21)_\ell$}$$
$$\cdots\cdots \tag*{$\cdots\cdot$}$$
$$(\beta + 1)\partial(p_{2k-1})\partial(p_{2k-2}) + \cdots + \partial(p_1) < Y, \tag*{$(4.21)_k$}$$
$$(\beta + 1)\partial(p_{2k+1}) + \partial(p_{2k}) + \cdots + \partial(p_1) \geq Y. \tag*{$(4.21)_{k+1}$}$$

Let

$$Q_s(x) := \begin{cases} x + x^2 + \cdots + x^s, & \text{if } s \text{ is a positive integer,} \\ 0, & \text{if } s = 0. \end{cases}$$

Then, from (4.21) we can deduce, by induction, that

$$\begin{aligned} &\beta\left(\partial(p_{2\ell}) + \partial(p_{2\ell-1}) + \cdots + \partial(p_2)\right) \\ &\quad \leq \quad (Y - \partial(p_1))\left[1 + 2Q_{\ell-1}\left(\frac{\beta - 1}{\beta + 1}\right)\right], \end{aligned} \tag{4.22}$$

for $1 \leq \ell \leq k$. Actually, from $(4.21)_1$, we have

$$\beta\partial(p_2) \leq \beta\partial(p_1) < Y - \partial(p_1),$$

and (4.22) is certainly true for $\ell = 1$. Then for $1 \leq \ell < k$, from $(4.21)_{\ell+1}$ and (4.22), we have

$$\begin{aligned} &(\beta + 1)\left(\partial(p_{2\ell+1}) + \partial(p_{2\ell}) + \cdots + \partial(p_2)\right) \\ &\quad < (Y - \partial(p_1)) + \beta\left(\partial(p_{2\ell}) + \cdots + \partial(p_2)\right) \\ &\quad \leq (Y - \partial(p_1)) + (Y - \partial(p_1))\left[1 + 2Q_{\ell-1}\left(\frac{\beta - 1}{\beta + 1}\right)\right], \end{aligned}$$

and thus

$$\partial(p_{2\ell+1}) + \partial(p_{2\ell}) + \cdots + \partial(p_2) \leq (Y - \partial(p_1)) \frac{2}{\beta+1} \left[1 + Q_{\ell-1}\left(\frac{\beta-1}{\beta+1}\right)\right].$$

Hence

$$\begin{aligned} &(\beta-1)\left(\partial(p_{2\ell+1}) + \partial(p_{2\ell}) + \cdots + \partial(p_2)\right) \\ &\quad \leq \ (Y - \partial(p_1)) \frac{2(\beta-1)}{\beta+1} \left[1 + Q_{\ell-1}\left(\frac{\beta-1}{\beta+1}\right)\right]. \end{aligned} \tag{4.23}$$

Now, $(4.21)_{\ell+1}$ implies

$$\beta\partial(p_{2\ell+2}) + \partial(p_{2\ell+1}) + \cdots + \partial(p_2) < Y - \partial(p_1), \tag{4.24}$$

since $\partial(p_{2\ell+2}) \leq \partial(p_{2\ell+1})$. It follows, from (4.23) and (4.24), that

$$\begin{aligned} &\beta\left(\partial(p_{2\ell+2}) + \partial(p_{2\ell+1}) + \cdots + \partial(p_2)\right) \\ &\quad < (Y - \partial(p_1)) \left[1 + \frac{2(\beta-1)}{\beta+1} + \frac{2(\beta-1)}{\beta+1} Q_{\ell-1}\left(\frac{\beta-1}{\beta+1}\right)\right] \\ &\quad = (Y - \partial(p_1)) \left[1 + 2Q_\ell\left(\frac{\beta-1}{\beta+1}\right)\right]. \end{aligned}$$

This proves (4.22).

We now obtain, from $(4.21)_{k+1}$ and (4.22) with $\ell = k$,

$$(\beta+1)\partial(p_{2k+1}) + \frac{Y - \partial(p_1)}{\beta}\left[1 + 2Q_{k-1}\left(\frac{\beta-1}{\beta+1}\right)\right] \geq Y - \partial(p_1),$$

and hence

$$\begin{aligned} \partial(p_{2k+1}) \ &\geq \ \frac{Y - \partial(p_1)}{\beta}\left[\frac{\beta-1}{\beta+1} - \frac{2}{\beta+1} Q_{k-1}\left(\frac{\beta-1}{\beta+1}\right)\right] \\ &= \ (Y - \partial(p_1)) \frac{1}{\beta}\left(\frac{\beta-1}{\beta+1}\right)^k. \end{aligned}$$

This proves (4.19).

Similarly, for $\bar{\chi}^-(d) = 1$,

$$d = p_1 p_2 \cdots p_{2k} \quad \text{with} \quad p_1 > p_2 > \cdots > p_{2k}$$

and, by (4.16) and (4.17), we have

$$\begin{array}{ll}
(\beta+1)\partial(p_2) + \partial(p_1) < Y, & (4.25)_1 \\
\cdots\cdots & \cdots\cdot \\
(\beta+1)\partial(p_{2k-2}) + \partial(p_{2k-3}) + \cdots + \partial(p_1) < Y, & (4.25)_{k-1} \\
(\beta+1)\partial(p_{2k}) + \partial(p_{2k-1}) + \cdots + \partial(p_1) \geq Y. & (4.25)_k
\end{array}$$

Let $Q_1^*(x) := x$ and

$$Q_s^*(x) := 2x + 2x^2 + \cdots + 2x^{s-1} + x^s, \quad s \geq 2.$$

Then, from (4.25), we can deduce, as before, that

$$\beta\left(\partial(p_{2\ell-1}) + \cdots + \partial(p_2)\right) \leq (Y - \partial(p_1))\left[1 + Q_{\ell-1}^*\left(\frac{\beta-1}{\beta+1}\right)\right], \tag{4.26}$$

for $2 \leq \ell \leq k$. From $(4.25)_k$ and (4.26) with $\ell = k$, we obtain

$$\begin{aligned}
\partial(p_{2k}) &\geq \frac{Y - \partial(p_1)}{\beta}\left[\frac{\beta-1}{\beta+1} - \frac{1}{\beta+1}Q_{k-1}^*\left(\frac{\beta-1}{\beta+1}\right)\right] \\
&= (Y - \partial(p_1))\frac{1}{\beta-1}\left(\frac{\beta-1}{\beta+1}\right)^k,
\end{aligned}$$

and (4.20) follows. □

(7.4.4) LEMMA. (Fundamental Lemma) *Assume that there exists a positive integer $n$ such that (4.6) holds for each divisor $d$ of $P_r^*$. Then, for any given positive number $L$ such that $L \geq 2$ and $Lr \leq n$, and any given $\varepsilon$ such that $0 < \varepsilon < 1$,*

$$S^{\pm} = O_\varepsilon\left(L^{-(1-\varepsilon)L}\right) \tag{4.27}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

*holds with* $Y = Lr$, $\beta = \max\{\varepsilon L, \beta_1\}$, *where* $\beta_1$ *is an absolute constant. Hence*

$$S(\mathcal{A}, \mathcal{P}^*, r) - Aq^n \left( \prod_{p | P_r^*} \left(1 - q^{-\partial(p)}\right) \right) \left\{1 + O_\varepsilon\left(L^{-(1-\varepsilon)L}\right)\right\} \\ \leq \sum_{\substack{d | P_r^* \\ \partial(d) < Lr}} \mu(d) \chi^+(d) R_d, \tag{4.28}$$

*and*

$$S(\mathcal{A}, \mathcal{P}^*, r) - Aq^n \left( \prod_{p | P_r^*} \left(1 - q^{-\partial(p)}\right) \right) \left\{1 + O_\varepsilon\left(L^{-(1-\varepsilon)L}\right)\right\} \\ \geq \sum_{\substack{d | P_r^* \\ \partial(d) < Lr}} \mu(d) \chi^-(d) R_d \tag{4.29}$$

*hold, with* $\chi^+(d)$ *and* $\chi^-(d)$ *defined in (4.14) and (4.16) respectively.*

Proof. Set $Y = Lr$ in Lemma 7.4.3, and in (4.15) and (4.17). First, note that $\chi^+(d) = 0$ for $\partial(d) \geq Lr$, by (4.15). Actually, if $\omega(d)$ is odd then $\eta^+(d) = 0$ by definition, and hence $\chi^+(d) = 0$. If $\omega(d)$ is even, then $\omega(d/\delta(d))$ is odd and

$$\beta\partial\left(\delta\left(\frac{d}{\delta(d)}\right)\right) + \partial\left(\frac{d}{\delta(d)}\right) \geq \partial(d) \geq Lr,$$

and thus $\eta^+(d/\delta(d)) = 0$, and hence $\chi^+(d) = 0$ too. Therefore the sum in the second term on the right-hand side of (4.7) becomes the sum on the right-hand side of (4.28). Thus, to prove (4.28), it is sufficient to obtain the estimate

$$S^+ = O_\varepsilon\left(L^{-(1-\varepsilon)L}\right)$$

for $S^+$ defined in (4.8).

From $(4.21)_{k+1}$ and (4.19), we obtain, for $\bar{\chi}^+(d) = 1$,

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

(i) $\beta\partial(\delta(d)) + \partial(d) \geq Lr$,

(ii) $\dfrac{Lr - \partial(\Delta(d))}{\partial(\delta(d))} \leq \beta \left(\dfrac{\beta+1}{\beta-1}\right)^{\omega(d)/2}$.

Hence, from (i),

$$r(\beta + \omega(d)) \geq Lr,$$

and then

$$\omega(d) \geq \max\{L - \beta, 1\}. \tag{4.30}$$

Also, from (ii),

$$\frac{(L-1)r}{\partial(\delta(d))} \leq \beta \left(\frac{\beta+1}{\beta-1}\right)^{\omega(d)/2},$$

and then

$$\frac{r}{\partial(\delta(d))} \leq \frac{\beta}{L-1} \left(\frac{\beta+1}{\beta-1}\right)^{\omega(d)/2}. \tag{4.31}$$

Note that

$$\begin{aligned}\prod_{\partial(\delta(d)) \leq \partial(p) \leq r} \left(1 - q^{-\partial(p)}\right)^{-1} &= \frac{\displaystyle\prod_{\partial(p) < \partial(\delta(d))} \left(1 - q^{-\partial(p)}\right)^{-1}}{\displaystyle\prod_{\partial(p) \leq r} \left(1 - q^{-\partial(p)}\right)^{-1}} \\ &\ll \frac{r}{\partial(\delta(d))} \left\{1 + O\left(\partial(\delta(d))^{-1}\right)\right\} \\ &\ll \frac{r}{\partial(\delta(d))},\end{aligned} \tag{4.32}$$

by (3.9) of Chapter 3. Therefore, from (4.32) and (4.31),

$$\prod_{\substack{\delta(d) \leq p \\ \partial(p) \leq r}} \left(1 - q^{-\partial(p)}\right)^{-1} \leq K \frac{\beta}{L-1} \left(\frac{\beta+1}{\beta-1}\right)^{\omega(d)/2}, \tag{4.33}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

with some constant $K$, for $\bar{\chi}^+(d) = 1$. Then, from (4.30) and (4.33), we obtain the estimate

$$|S^+| \le K \frac{\beta}{L-1} \sum_{\substack{d|P_r^* \\ \omega(d) \ge \max\{L-\beta, 1\}}} \bar{\chi}^+(d) q^{-\partial(d)} \beta_0^{\omega(d)}, \tag{4.34}$$

with

$$\beta_0 = \left( \frac{\beta+1}{\beta-1} \right)^{\frac{1}{2}}.$$

Toward the sum on the right–hand side of (4.34), the contribution of those terms with $\omega(d) = k$ is, by (4.33) and Stirling's formula,

$$\begin{aligned}
&\le \beta_0^k \sum_{\substack{d|P_r^* \\ \omega(d)=k}} \bar{\chi}^+(d) q^{-\partial(d)} \le \beta_0^k \frac{1}{k!} \left( \sum_{\partial\left(\delta(d_0)\right) \le \partial(p) \le r} q^{-\partial(p)} \right)^k \\
&\le \beta_0^k \frac{1}{k!} \left[ \log \left( \prod_{\partial\left(\delta(d_0)\right) \le \partial(p) \le r} \left(1 - q^{-\partial(p)}\right)^{-1} \right) \right]^k \\
&\le \beta_0^k \frac{1}{k!} \left[ \log \left( 2KL^{-1}\beta\beta_0^k \right) \right]^k \\
&\le \left[ \beta_0 e \left( k^{-1} \log(2KL^{-1}\beta) + \log \beta_0 \right) \right]^k,
\end{aligned}$$

where $d_0$ is a divisor of $P_r^*$ such that $\bar{\chi}^+(d_0) = 1$, $\omega(d_0) = k$, and

$$\delta(d_0) = \min \left\{ \delta(d) : \, d \mid P_r^*, \, \bar{\chi}^+(d) = 1, \, \omega(d) = k \right\}.$$

Thus, we obtain

$$|S^+| \le K \frac{\beta}{L-1} \sum_{k \ge \max\{L-\beta, 1\}} \zeta_k^k,$$

where

$$\zeta_k = \beta_0 e \left( k^{-1} \log(2KL^{-1}\beta) + \log \beta_0 \right).$$

If $L$ is large, $L \ge L_0(K, \varepsilon)$, let $\beta = \alpha L$ with $0 < \alpha < \min\left\{\frac{1}{2}, \varepsilon\right\}$. Then

$$\log \beta_0 = \frac{1}{2} \log \left( 1 + \frac{2}{\beta - 1} \right) \le \frac{2}{\beta},$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

and we have

$$\begin{aligned}\zeta_k &\leq \beta_0 e\left(k^{-1}\log(2K\alpha)+2(\alpha L)^{-1}\right)\\ &\leq \beta_0 e\left(\frac{\log(2K\alpha)}{(1-\alpha)L}+\frac{2}{\alpha L}\right)\leq\frac{C_1}{L},\end{aligned}$$

since $k \geq L-\beta=(1-\alpha)L$ and $\beta_0<2$. Therefore we obtain

$$\begin{aligned}|S^{+}| &\leq K\frac{\alpha L}{L-1}\sum_{k\geq(1-\alpha)L}\left(\frac{C_1}{L}\right)^k\\ &\leq K\frac{\alpha L}{L-1}\left(\frac{C_1}{L}\right)^{(1-\alpha)L}\left(1-\frac{C_1}{L}\right)^{-1}=O_\varepsilon\left(L^{-(1-\varepsilon)L}\right).\end{aligned}$$

If $L$ is small, $L<L_0(K,\varepsilon)$, choose $\beta$ so large that $e\beta_0\log\beta_0<\frac{1}{3}$. Then

$$\zeta_k=\beta_0 e k^{-1}\log\left(2KL^{-1}\beta\right)+e\beta_0\log\beta_0<\frac{2}{3}$$

for $k\geq k_0$. We obtain

$$|S^{+}|\leq\frac{K\beta}{L-1}\left(\sum_{k<k_0}\zeta_k^k+\sum_{k\geq k_0}\left(\frac{2}{3}\right)^k\right)\ll_\varepsilon 1.$$

This proves (4.28).

Similarly, $\chi^{-}(d)=0$ for $\partial(d)\geq Lr$, by (4.17). The sum in the second term on the right–hand side of (4.9) is zero, and the last sum of (4.9) becomes the right–hand side of (4.29). From $(4.25)_k$ and (4.20), (i) and (ii) hold for $\bar{\chi}^{-}(d)=1$ too. An argument similar to the one given above yields the estimate

$$|S^{-}|\leq O_\varepsilon\left(L^{-(1-\varepsilon)L}\right),$$

and (4.29) follows. □

(7.4.5) LEMMA. *Assume that there exist constants $A>0$, $q>1$, and $\gamma>1$ such that (3.1) holds, and such that, in addition to (4.6),*

$$R_d=O\left(q^{n-\partial(d)}(n-\partial(d))^{-\gamma}\right) \tag{4.35}$$

*holds for $\partial(d) < n/k$ with $k > 1$. Then, for any given number $L$ such that $L \geq 2$ and $Lr \leq n/k$,*

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}^*, r) &= Aq^n \left( \prod_{p \mid P_r^*} \left(1 - q^{-\partial(p)}\right) \right) \\ &\quad \times \left\{ 1 + O_\varepsilon\left(L^{-(1-\varepsilon)L}\right) + O_k\left(r^2 n^{-\gamma}\right) \right\}. \qquad (4.36) \end{aligned}$$

PROOF. We have

$$\begin{aligned} \sum_{\substack{d \mid P_r^* \\ \partial(d) < Lr}} \mu(d) \chi^{\pm}(d) R_d &\ll \sum_{\substack{d \mid P_r^* \\ \partial(d) < n/k}} q^{n - \partial(d)} (n - \partial(d))^{-\gamma} \\ &\ll_k n^{-\gamma} q^n \sum_{d \mid P_r^*} q^{-\partial(d)} \\ &= n^{-\gamma} q^n \prod_{p \mid P_r^*} \left(1 + q^{-\partial(p)}\right), \end{aligned}$$

and hence

$$\begin{aligned} & q^{-n} \prod_{p \mid P_r^*} \left(1 - q^{-\partial(p)}\right)^{-1} \sum_{\substack{d \mid P_r^* \\ \partial(d) < Lr}} \mu(d) \chi^{\pm}(d) R_d \\ &\ll_k n^{-\gamma} \prod_{p \mid P_r^*} \left(1 + q^{-\partial(p)}\right) \left(1 - q^{-\partial(p)}\right)^{-1} \\ &\leq n^{-\gamma} \prod_{p \mid P_r^*} \left(1 - q^{-\partial(p)}\right)^{-2} \\ &\ll r^2 n^{-\gamma}, \end{aligned}$$

by (3.9) of Chapter 3. □

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

## 7.5 A Probability Model

As in the classical probabilistic number theory, a probability model will clarify the idea of the proofs of the main theorems, given in the next section.

Let $f$ be a real-valued strongly additive function on an arithmetical semigroup $\mathcal{G}$. Let $r$ and $m$ be positive integers with $r < m$. In the proofs, we shall use, instead of $f$, the function $f_r$ such that

$$f_r(a) = \sum_{\substack{p|a \\ \partial(p) \leq r}} f(p),$$

a truncation of $f$. Here, as usual, the sum in the definition is assumed zero when the number of summands is zero. Note that $f_r$ is strongly additive, and $f_r(a) = f(a)$ when $\partial(a) \leq r$. Consider $\Omega := \{a : a \in \mathcal{G}, \partial(a) = m\}$. The range of $f_r$ on $\Omega$ is a finite set $\{x_1, \ldots, x_t\}$, say. The subsets $\{a : \partial(a) = m, f_r(a) = x_i\}$, $i = 1, \ldots, t$ of $\Omega$ are pairwaise disjoint. Let $P_r := \prod_{\partial(p) \leq r} p$. Then,

$$\{a : \partial(a) = m, f_r(a) = x_i\} = \bigcup_{\substack{g|P_r \\ f(g) = x_i}} E_g,$$

where the subset

$$E_g := \{a : \partial(a) = m, g \mid a, (a, P_r/g) = 1\}.$$

For $a \in \Omega$, if $g$ is the greatest common divisor (in the sense defined in a free commutative semigroup) of $a$ and $P_r$, then $a \in E_g$. Hence the class of non-empty sets $E_g$ for divisors of $P_r$ forms a partition of $\Omega$. Let $\mathcal{E} = \{g : g \mid P_r, E_g \neq \phi\}$. The ($\sigma-$) field $\mathcal{F}$ generated by this partition consists of unions $E$ of a finite number of sets $E_g$, with $g \in \mathcal{E}$. Define an additive set function $\nu(E)$ on $\mathcal{F}$ by setting

$$\nu(E_g) = \frac{|E_g|}{G(m)},$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

where $|E_g|$ is the cardinality of $E_g$. Then $\nu$ is a probability measure on $\mathcal{F}$.

We now use the fundamental lemma (Lemma 7.4.5) to analyze the measure $\nu$.

(7.5.1) LEMMA. *Suppose that*

$$G(n) = Aq^n + O\left(q^n n^{-\gamma}\right), \quad n \geq 1 \tag{5.1}$$

*holds, with* $A > 0$, $q > 1$ *and* $\gamma > 1$, *and that* $\frac{r}{m} = o(1)$ *as* $m \to \infty$. *Then, for divisors* $g$ *of* $P_r$ *with* $\partial(g) \leq \frac{m}{2}$,

$$|E_g| = Aq^{m-\partial(g)} \left( \prod_{p|(P_r/g)} \left(1 - q^{-\partial(p)}\right) \right) \left[1 + O\left(r^2(m^{-2} + m^{-\gamma})\right)\right]. \tag{5.2}$$

PROOF. Let

$$L = 5\left(\log \frac{m}{r}\right)\left(\log\log \frac{m}{r}\right)^{-1}. \tag{5.3}$$

Then

$$\frac{Lr}{m} = o(1)$$

as $m \to \infty$. For $m$ sufficiently large,

$$Lr \leq 2^{-1}(m - \partial(g)) \quad \left(\geq 4^{-1}m\right).$$

Let

$$\mathcal{A} := \{a : \partial(a) = m, \, g \mid a\},$$

and $\mathcal{P}^* := \{p : (p, g) = 1\}$. Then

$$|E_g| = S(\mathcal{A}, \mathcal{P}^*, r)$$

and, for divisors $d$ of $P_r^*$ with $\partial(d) < m - \partial(g)$,

$$\begin{aligned} |\mathcal{A}_d| &= \Big|\{a : \partial(a) = m, \, gd \mid a\}\Big| = G(m - \partial(g) - \partial(d)) \\ &= Aq^{m-\partial(g)-\partial(d)} + O\left(q^{m-\partial(g)-\partial(d)}(m - \partial(g) - \partial(d))^{-\gamma}\right). \end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

By Lemma 7.4.5, with $n = m - \partial(g)$, $L$ given by (5.3), $k = 2$, and $\varepsilon = \frac{1}{2}$, we have

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}^*, r) &= Aq^{m-\partial(g)} \left( \prod_{p|(P_r/g)} \left(1 - q^{-\partial(p)}\right) \right) \\ &\quad \times \left[1 + O\left(r^2(m^{-2} + m^{-\gamma})\right)\right], \end{aligned}$$

and (5.2) follows. □

Then, by (5.2),

$$\nu(E_g) = q^{-\partial(g)} \left( \prod_{p|(P_r/g)} \left(1 - q^{-\partial(p)}\right) \right) \left[1 + O\left(r^2(m^{-2} + m^{-\gamma})\right)\right].$$

Let $\mu_g := q^{-\partial(g)} \prod_{p|(P_r/g)} \left(1 - q^{-\partial(p)}\right)$. Thus $\mu_g$ is a good approximation of $\nu(E_g)$ for divisors $g$ of $P_r$ with $\partial(g) \leq \frac{m}{2}$, provided that $\gamma \geq 2$ $\left(\frac{r}{m} = o(1)!\right)$. The following lemma shows that $\mu_g$, $g \mid P_r$, is a probability density.

(7.5.2) Lemma. *We have*

$$\sum_{g|P_r} q^{-\partial(g)} \prod_{p|(P_r/g)} \left(1 - q^{-\partial(p)}\right) = 1. \tag{5.4}$$

Proof. We may write the left–hand side in the form

$$\left( \prod_{p|P_r} \left(1 - q^{-\partial(p)}\right) \right) \left( \sum_{g|P_r} q^{-\partial(g)} \prod_{p|g} \left(1 - q^{-\partial(p)}\right)^{-1} \right). \tag{5.5}$$

The second factor equals

$$\sum_{g|P_r} q^{-\partial(g)} \prod_{p|g} \sum_{k=0}^{\infty} q^{-k\partial(p)} = \sum_{g|P_r} q^{-\partial(g)} \sum_{k(b)|g} q^{-\partial(b)},$$

where $k(b)$ denotes the product of distinct prime divisors of $b$. Hence the second factor of (5.5) equals

$$\sum_{k(a)|P_r} q^{-\partial(a)} = \prod_{p|P_r} \left(1 - q^{-\partial(p)}\right)^{-1}.$$

Then (5.4) follows. □

Therefore we may anticipate that the density $\mu_g$, $g \mid P_r$, leads to a good approximation of $\nu(E)$ on $\mathcal{F}$.

(7.5.3) LEMMA. *Let*

$$h(d) := q^{\partial(d)} \prod_{p|d} \left(1 - q^{-\partial(p)}\right),$$

*and*

$$s := \sum_{p|P_r} \partial(p) q^{-\partial(p)}.$$

*Then, for* $n > es$,

$$\sum_{\substack{d|P_r \\ \partial(d)\geq n}} \frac{1}{h(d)} \leq \left(\prod_{p|P_r} \left(1 - q^{-\partial(p)}\right)^{-1}\right) \exp\left\{-nr^{-1}\Delta\right\}, \tag{5.6}$$

*where*

$$\Delta = \log\left(ns^{-1}\right) - \log\log\left(ns^{-1}\right) - 1.$$

PROOF. We have

$$\begin{aligned}
\sum_{d|P_r} \frac{q^{\lambda\partial(d)}}{h(d)} &= \prod_{p|P_r} \left(1 + \frac{q^{\lambda\partial(p)}}{h(p)}\right) \\
&= \prod_{p|P_r} \left(1 + q^{-\partial(p)} \left(1 - q^{-\partial(p)}\right)^{-1} q^{\lambda\partial(p)}\right) \\
&= \prod_{p|P_r} \left(1 - q^{-\partial(p)}\right)^{-1} \prod_{p|P_r} \left(1 + q^{-\partial(p)} \left(q^{\lambda\partial(p)} - 1\right)\right).
\end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Since $1+t \leq e^t$, and $e^t - 1 \leq te^t$, when $t \geq 0$,

$$\begin{aligned}
&\prod_{p|P_r} \left(1 + q^{-\partial(p)}\left(q^{\lambda\partial(p)} - 1\right)\right) \\
&\quad \leq \exp\left\{\sum_{p|P_r} q^{-\partial(p)}\left(q^{\lambda\partial(p)} - 1\right)\right\} \\
&\quad \leq \exp\left\{\lambda \sum_{p|P_r} q^{-\partial(p)}\partial(p)q^{\lambda\partial(p)} \log q\right\} \\
&\quad \leq \exp\left\{\lambda q^{\lambda r} s \log q\right\}.
\end{aligned}$$

Let $\lambda = \frac{\rho}{r \log q}$. Then

$$\begin{aligned}
\sum_{\substack{d|P_r \\ \partial(d)\geq n}} \frac{1}{h(d)} &\leq \sum_{d|P_r} \frac{1}{h(d)}\left(\frac{q^{\partial(d)}}{q^n}\right)^{\lambda} \\
&\leq \prod_{p|P_r}\left(1 - q^{-\partial(p)}\right)^{-1} \exp\left\{\lambda(se^{\rho} - n)\log q\right\} \\
&= \prod_{p|P_r}\left(1 - q^{-\partial(p)}\right)^{-1} \exp\left\{sr^{-1}\rho(e^{\rho} - ns^{-1})\right\}.
\end{aligned}$$

Let $\rho = \log(ns^{-1}) - \log\log(ns^{-1})$. Since $ns^{-1} > e$, $\rho > 0$. Then

$$\begin{aligned}
\rho(e^{\rho} - ns^{-1}) &= -ns^{-1}\Bigg(\log(ns^{-1}) - \log\log(ns^{-1}) \\
&\qquad + \frac{\log\log(ns^{-1})}{\log(ns^{-1})} - 1\Bigg),
\end{aligned}$$

and (5.6) follows. □

From (5.6), we obtain the estimate

$$\begin{aligned}
&\sum_{\substack{d|P_r \\ \partial(d)\geq n}} q^{-\partial(d)} \prod_{p|(P_r/d)}\left(1 - q^{-\partial(p)}\right) \\
&\quad = \prod_{p|P_r}\left(1 - q^{-\partial(p)}\right) \sum_{\substack{d|P_r \\ \partial(d)\geq n}} \frac{1}{h(d)} \leq \exp\left\{-nr^{-1}\Delta\right\}. \qquad (5.7)
\end{aligned}$$

(7.5.4) LEMMA. *Suppose that (5.1) holds with $A > 0$, $q > 1$, and $\gamma = 2$, and that $\frac{r}{m} = o(1)$ as $m \to \infty$. Then, for $E \in \mathcal{F}$, $E = \cup_{1 \le j \le k} E_{g_j}$, where $E_{g_j} \ne \emptyset$, and $g_j \ne g_j$ for $i \ne j$, we have*

$$\nu(E) = \sum_{j=1}^{k} q^{-\partial(g_j)} \prod_{p|(P_r/g_j)} \left(1 - q^{-\partial(p)}\right) + O\left(r^2 m^{-2}\right). \tag{5.8}$$

PROOF. We have

$$\nu(E) = \sum_{j=1}^{k} \frac{\left|E_{g_j}\right|}{G(m)} = \left( \sum_{\substack{1 \le j \le k \\ \partial(g_j) \le \frac{m}{2}}} + \sum_{\substack{1 \le j \le k \\ \partial(g_j) > \frac{m}{2}}} \right) \frac{\left|E_{g_j}\right|}{G(m)} = S_1 + S_2,$$

say. By Lemma 7.5.1,

$$S_1 = \left\{1 + O\left(r^2 m^{-2}\right)\right\} \sum_{\substack{1 \le j \le k \\ \partial(g_j) \le \frac{m}{2}}} q^{-\partial(g_j)} \prod_{p|(P_r/g_j)} \left(1 - q^{-\partial(p)}\right).$$

To evaluate $S_2$, we apply (5.7) with $n = \left[\frac{m+1}{2}\right]$. Note that

$$\sum_{p|P_r} \partial(p) q^{-\partial(p)} = \sum_{\partial(p) \le r} \partial(p) q^{-\partial(p)} = r + O(1),$$

by (3.8) of Chapter 3. Hence, in (5.7),

$$n s^{-1} = \frac{\left[\frac{m+1}{2}\right]}{r + O(1)} = (1 + O(1)) \frac{m}{2r},$$

and

$$\Delta = (1 + o(1)) \log \frac{m}{2r}.$$

Then

$$\begin{aligned} S_2 &\le \sum_{\substack{g|P_r \\ \partial(g)>\frac{m}{2}}} \frac{|E_g|}{G(m)} = 1 - \sum_{\substack{g|P_r \\ \partial(g)\le\frac{m}{2}}} \frac{|E_g|}{G(m)} \\ &= 1 - \left\{1 + O(r^2m^{-2})\right\} \sum_{\substack{g|P_r \\ \partial(g)\le\frac{m}{2}}} q^{-\partial(g)} \prod_{p|(P_r/g)} \left(1 - q^{-\partial(p)}\right) \\ &= \sum_{\substack{g|P_r \\ \partial(g)>\frac{m}{2}}} \mu_g + O(r^2m^{-2}), \end{aligned}$$

by Lemma 7.5.2. Then, by (5.7),

$$\begin{aligned} S_2 &= O\left(\exp\left\{-(1+o(1))m(2r)^{-1}\log\left(m(2r)^{-1}\right)\right\}\right) + O(r^2m^{-2}) \\ &= O(r^2m^{-2}). \end{aligned}$$

Therefore

$$\begin{aligned} \nu(E) &= \sum_{\substack{1\le j\le k \\ \partial(g_j)\le\frac{m}{2}}} q^{-\partial(g_j)} \prod_{p|(P_r/g_j)} \left(1 - q^{-\partial(p)}\right) + O(r^2m^{-2}) \\ &= \sum_{j=1}^{k} q^{-\partial(g_j)} \prod_{p|(P_r/g_j)} \left(1 - q^{-\partial(p)}\right) + O(r^2m^{-2}), \end{aligned}$$

by (5.7) again. □

If we let

$$\mu(E) = \sum_{j=1}^{k} q^{-\partial(g_j)} \prod_{p|(P_r/g_j)} \left(1 - q^{-\partial(p)}\right) = \sum_{j=1}^{k} \mu_{g_j}$$

for $E = \cup_{1\le j\le k} E_{g_j}$, then Lemma 7.5.4 shows that $\mu(E)$ is a good approximation of $\nu(E)$, provided that $\frac{r}{m} = o(1)$ as $m \to \infty$. Unfortunately, $\mu$ is not a probability measure on $\mathcal{F}$. To see this, we note that for some divisors $g$ of $P_r$ the sets $E_g$ are empty. If $\mu$ were a measure, we would have $\mu(E_g) = 0$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

(instead of $\mu(E_g) = \mu_g!$) for those $E_g$, which would imply $\mu(\Omega) < 1$ (see Lemma 7.5.2).

Therefore, in the proof of Theorem 7.6.1 of the next section, we have to appeal to *another* probability space, on which there exists an independent sequence of random variables such that the distribution of their sum has the density $\mu_g$.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

## 7.6 Infinitely Divisible Distributions and a Central Limit Theorem

Let $f$ be a real–valued strongly additive arithmetical function on an arithmetical semigroup $\mathcal{G}$, and

$$\bar{\mu}(x) := \sum_{\partial(p)\leq x} f(p)q^{-\partial(p)},$$

$$\sigma(x) := \left(\sum_{\partial(p)\leq x} f^2(p)q^{-\partial(p)}\right)^{\frac{1}{2}}$$

(see (3.18) and (3.19)). Following Kubilius [1] (cf. also Elliott [1]), we shall say that $f$ *belongs to the class* $H$ if and only if there exists a function $r = r(x)$ such that

$$\frac{r}{x} \to 0, \quad \frac{\sigma(r)}{\sigma(x)} \to 1, \quad \sigma(x) \to \infty, \tag{6.1}$$

as $x \to \infty$.

We shall now prove a main theorem, Theorem 7.6.1, an analogue of the *Kubilius Main Theorem* (Kubilius [1], Elliott [1]). For convenience, let $P(a, x, m)$ denote a proposition on elements $a$ in $\mathcal{G}$, with parameters $x$ and $m$, and let

$$\nu_m(P(a, x, m)) := \sum_{\substack{\partial(a)=m\\ P(a,x,m)}} 1 \tag{6.2}$$

be the number of true values of $P(a, x, m)$ among those $a$ with $\partial(a) = m$.

(7.6.1) THEOREM. (cf. Zhang [3]) *Suppose that there exist constants* $A > 0$, $q > 1$ *and* $c \geq 0$, *such that*

$$|G(n) - Aq^n| \leq cq^n n^{-2}, \quad n = 1, 2, \ldots . \tag{6.3}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

*Let $f$ be a real-valued strongly additive function of class $H$. Then the relative frequency*

$$\frac{1}{G(m)}\nu_m\left(f(a)-\bar{\mu}(m)\leq x\sigma(m)\right) \tag{6.4}$$

*converges weakly to a limit distribution as $m\to\infty$ if and only if there exists a distribution function $K(x)$ such that*

$$\frac{1}{\sigma^2(m)}\sum_{\substack{\partial(p)\leq m\\ f(p)\leq x\sigma(m)}} f^2(p)q^{-\partial(p)}\to K(x) \tag{6.5}$$

*weakly as $m\to\infty$. Moreover, the limit distribution has mean zero, variance 1, and characteristic function $\phi(t)$ given by*

$$\log\phi(t)=\int_{-\infty}^{\infty}\left(e^{itx}-1-itx\right)x^{-2}dK(x). \tag{6.6}$$

*In addition, whether (6.4) converges or not,*

$$\frac{1}{G(m)\sigma(m)}\sum_{\partial(a)=m}\left(f(a)-\bar{\mu}(m)\right)\to 0, \tag{6.7}$$

*and*

$$\frac{1}{G(m)\sigma^2(m)}\sum_{\partial(a)=m}\left(f(a)-\bar{\mu}(m)\right)^2\to 1 \tag{6.8}$$

*as $m\to\infty$.*

To prove Theorem 7.6.1, we introduce a finite sequence $\{X_p,\ \partial(p)\leq r\}$ of independent random variables on some probability space such that

$$X_p=\begin{cases} f(p), & \text{with probability } q^{-\partial(p)},\\ 0, & \text{with probability } 1-q^{-\partial(p)}.\end{cases}$$

By Lemma 7.1.2, such a sequence $\{X_p,\ \partial(p)\leq r\}$ exists. The following lemma shows that the sum $\sum_{\partial(p)\leq r}X_p$ and the function $f_r(a)$ have the same limit distribution function as $m\to\infty$.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

(7.6.2) LEMMA. *Let $r = r(m)$ be defined as in (6.1). Let $P$ be the probability measure of the probability space on which $X_p$, $\partial(p) \leq r$ are defined. Then*

$$\begin{aligned}&\frac{1}{G(m)}\nu_m\left(f_r(a) - \bar{\mu}(r) \leq x\sigma(r)\right)\\ &\quad = P\left[\sum_{\partial(p)\leq r} X_p - \bar{\mu}(r) \leq x\sigma(r)\right] + O(r^2m^{-2}) \qquad (6.9)\end{aligned}$$

*uniformly for $-\infty < x < \infty$ and $m \in \mathbb{N}$.*

PROOF. Let

$$E := \left\{a : \partial(a) = m,\, f_r(a) - \bar{\mu}(r) \leq x\sigma(r)\right\}.$$

Then the left–hand side of (6.9) is just $\nu(E)$. We claim that

$$\nu(E) = P\left[\sum_{\partial(p)\leq r} X_p - \bar{\mu}(r) \leq x\sigma(r)\right] - \sum_{\substack{g|P_r,\, g\notin\mathcal{E}\\ \{(\})\leq\not{\bar\mu}(\nabla)+\S\sigma(\nabla)}} \mu_g + O(r^2m^{-2}). \qquad (6.10)$$

Actually, if $E$ is non–empty, then

$$E = \bigcup_{\substack{g\in\mathcal{E}\\ \{(\})\leq\not{\bar\mu}(\nabla)+\S\sigma(\nabla)}} E_g,$$

where $\mathcal{E}$ is the set of $g$ such that $g \mid P_r$, and such that $E_g \neq \emptyset$ (see Section 7.5). By Lemma 7.5.4,

$$\nu(E) = \sum_{\substack{g\in\mathcal{E}\\ \{(\})\leq\not{\bar\mu}(\nabla)+\S\sigma(\nabla)}} \mu_g + O(r^2m^{-2}),$$

where

$$\mu_g = q^{-\partial(g)} \prod_{p|(P_r/g)} \left(1 - q^{-\partial(p)}\right).$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Note that

$$
\begin{aligned}
&P\left[\sum_{\partial(p)\le r} X_p - \bar{\mu}(r) \le x\sigma(r)\right] \\
&\quad = P\left[\bigcup_{\substack{g|P_r \\ f(g)\le\bar{\mu}(r)+x\sigma(r)}} \Big(\{X_p = f(p),\, p \mid g\} \cap \{X_p = 0,\, (p,g) = 1,\, \partial(p) \le r\}\Big)\right] \\
&\quad = \sum_{\substack{g|P_r \\ f(g)\le\bar{\mu}(r)+x\sigma(r)}} \mu_g .
\end{aligned}
$$

Hence (6.10) holds. If $E$ is empty, then

$$
P\left[\sum_{\partial(p)\le r} X_p - \bar{\mu}(r) \le x\sigma(r)\right] = \sum_{\substack{g|P_r,\, g\notin\mathcal{E} \\ \{()\}\le\not{\mu}(\nabla)+\S\sigma(\nabla)}} \mu_g ,
$$

and (6.10) holds plainly.

Now, if $g$ is a divisor of $P_r$ and $g \notin \mathcal{E}$, then $E_g = \{a : \partial(a) = m,\, g \mid a,\, (a, P_r/g) = 1\} = \emptyset$, and hence $\partial(g) > \frac{m}{2}$ by Lemma 7.5.1. By (5.7),

$$
\sum_{\substack{g|P_r,\, g\notin\mathcal{E} \\ \{()\}\le\not{\mu}(\nabla)+\S\sigma(\nabla)}} \mu_g \le \sum_{\substack{g|P_r \\ \partial(g)>\frac{m}{2}}} \mu_g = O\left(\exp\left\{-(1+o(1))\frac{m}{2r}\log\frac{m}{2r}\right\}\right). \quad (6.11)
$$

Then (6.9) follows from (6.10) and (6.11). □

PROOF OF THEOREM 7.6.1. We define, by truncation, the strongly additive function $f_r$ such that

$$
f_r(a) = \sum_{\substack{p|a \\ \partial(p)\le r}} f(p),
$$

where $r = r(m)$ is defined in (6.1). Accordingly, define

$$\bar{\mu}_r(x) = \sum_{\partial(p) \le x} f_r(p) q^{-\partial(p)},$$

and

$$\sigma_r(x) = \left( \sum_{\partial(p) \le x} f_r^2(p) q^{-\partial(p)} \right)^{\frac{1}{2}}.$$

Thus $\bar{\mu}_r(x) = \bar{\mu}(r)$ and $\sigma_r(x) = \sigma(r)$ for $x \ge r$. Then, for each fixed $\varepsilon > 0$,

$$\frac{1}{G(m)} \nu_m \left( \left| (f(a) - f_r(a)) - (\bar{\mu}(m) - \bar{\mu}_r(m)) \right| \ge \varepsilon \sigma(m) \right)$$

$$\le \frac{1}{G(m) \varepsilon^2 \sigma^2(m)} \sum_{\partial(a) = m} \left[ \sum_{\substack{p \mid a \\ r < \partial(p) \le m}} f(p) - (\bar{\mu}(m) - \bar{\mu}_r(m)) \right]^2,$$

by an analogue of Chebyshev's inequality. By Lemma 7.3.6, the right-hand side is

$$\ll \frac{1}{\varepsilon^2 \sigma^2(m)} \left( \sum_{r < \partial(p) \le m} f^2(p) q^{-\partial(p)} \right) = \frac{\sigma^2(m) - \sigma^2(r)}{\varepsilon^2 \sigma^2(m)} = o_\varepsilon(1),$$

since $f$ is of class $H$. This implies that

$$\frac{(f(a) - f_r(a)) - (\bar{\mu}(m) - \bar{\mu}_r(m))}{\sigma(m)}$$

converges to 0 in distribution. By Lemma 7.1.5, the relative frequency (6.4) converges weakly to a distribution function $F(x)$ as $m \to \infty$ if and only if

$$\frac{1}{G(m)} \nu_m \left( f_r(a) - \bar{\mu}_r(m) \le x \sigma(m) \right) \tag{6.12}$$

converges weakly to the same function $F(x)$. Since $\sigma_r(m)/\sigma(m) = \sigma(r)/\sigma(m)$ $\to 1$ as $m \to \infty$, by Lemma 7.1.5 again, it turns out that (6.12) converges weakly to $F(x)$, and hence (6.4) does too, if and only if so does

$$\frac{1}{G(m)} \nu_m \left( f_r(a) - \bar{\mu}_r(m) \le x \sigma_r(m) \right).$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

By Lemma 7.6.2,

$$\begin{aligned}
&\frac{1}{G(m)}\nu_m\left(f_r(a) - \bar{\mu}_r(m) \le x\sigma_r(m)\right)\\
&\quad = P\left[\sum_{\partial(p)\le r} X_p - \bar{\mu}(r) \le x\sigma(r)\right] + O(r^2m^{-2})
\end{aligned}$$

uniformly for $-\infty < x < \infty$, and $m \in \mathbb{N}$. Since $\frac{r}{m} \to 0$ as $m \to \infty$, it follows that (6.4) converges weakly to a distribution function $F(x)$ as $m \to \infty$ if and only if

$$P\left[\sum_{\partial(p)\le r} X_p - \bar{\mu}(r) \le x\sigma(r)\right] \tag{6.13}$$

converges weakly to the same $F(x)$.

Now the distribution function (6.13) has the characteristic function

$$\phi_m(t) = e^{it\bar{\mu}(r)/\sigma(r)} \prod_{\partial(p)\le r}\left(1 + q^{-\partial(p)}\left(e^{itf(p)/\sigma(r)} - 1\right)\right),$$

since $X_p$, $\partial(p) \le r$ are independent. Hence

$$\log\phi_m(t) = -it\frac{\bar{\mu}(r)}{\sigma(r)} + \sum_{\partial(p)\le r} q^{-\partial(p)}\left(e^{itf(p)/\sigma(r)} - 1\right) + \eta_m(t),$$

where

$$\eta_m(t) = \sum_{\partial(p)\le r}\left\{\log\left(1 + q^{-\partial(p)}\left(e^{itf(p)/\sigma(r)} - 1\right)\right) - q^{-\partial(p)}\left(e^{itf(p)/\sigma(r)} - 1\right)\right\}.$$

We have

$$\begin{aligned}
|\eta_m(t)| \le \sum_{\partial(p)\le r_0}&\left|\log\left(1 + q^{-\partial(p)}\left(e^{itf(p)/\sigma(r)} - 1\right)\right)\right.\\
&\left.-q^{-\partial(p)}\left(e^{itf(p)/\sigma(r)} - 1\right)\right| + 2\sum_{r_0\le\partial(p)<r} q^{-2\partial(p)}.
\end{aligned}$$

The last sum equals

$$\sum_{n=r_0}^{r} q^{-2n}P(n) \ll \sum_{n=r_0}^{r} q^{-n}n^{-1} \le \frac{1}{r_0}\frac{q^{-r_0}}{1-q^{-1}},$$

since $P(n) \ll q^n n^{-1}$. Given $\varepsilon > 0$, we fix $r_0$ so that

$$\frac{1}{r_0}\frac{q^{-r_0}}{1-q^{-1}} < \varepsilon.$$

Then, for $m$ sufficiently large, $r = r(m) > r_0$, we have

$$\begin{aligned} |\eta_m(t)| \quad \le \quad & \varepsilon + \sum_{\partial(p)\le r_0} \Big|\log\left(1 + q^{-\partial(p)}\left(e^{itf(p)/\sigma(r)} - 1\right)\right) \\ & -q^{-\partial(p)}\left(e^{itf(p)/\sigma(r)} - 1\right)\Big|. \end{aligned}$$

It follows that

$$\limsup_{m\to\infty} |\eta_m(t)| \le \varepsilon,$$

and hence, letting $\varepsilon \to 0$,

$$\lim_{m\to\infty} |\eta_m(t)| = 0.$$

Thus

$$\log \phi_m(t) = \int_{-\infty}^{\infty} \left(e^{itu} - 1 - itu\right) u^{-2} dK(r,u) + o(1)$$

as $m \to \infty$, where

$$K(r,u) = \frac{1}{\sigma^2(r)} \sum_{\substack{\partial(p)\le r \\ f(p)\le u\sigma(r)}} f^2(p)q^{-\partial(p)}.$$

Note that $K(r,u)$ is a distribution function of $u$. Now, by Lemma 7.1.7, the Kolmogorov theorem,

$$\bar{\phi}_m(t) = \exp\left\{\int_{-\infty}^{\infty} \left(e^{itu} - 1 - itu\right) u^{-2} dK(r,u)\right\}$$

is the characteristic function of an infinitely divisible distribution. It follows, by Lemma 7.1.8, that (6.4) converges weakly to a limit distribution

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

function $F(x)$ if and only if there exists a distribution function $K(u)$ such that $K(r,u) \Longrightarrow K(u)$ as $r \to \infty$. This proves the main part of Theorem 7.6.1.

To prove (6.8), we note, from the proof given above, that

$$\sum_{\partial(a)=m} \left[(f(a)-f_r(a))-(\bar{\mu}(m)-\bar{\mu}_r(m))\right]^2 = o\left(q^m\sigma^2(m)\right).$$

It is sufficient to show that

$$\frac{1}{G(m)\sigma^2(m)} \sum_{\partial(a)=m} (f_r(a)-\bar{\mu}(r))^2 \to 1 \tag{6.14}$$

as $m \to \infty$. The last sum can be rewritten as

$$\sum_{\partial(a)=m} f_r^2(a) - 2\bar{\mu}(r) \sum_{\partial(a)=m} f_r(a) + G(m)(\bar{\mu}(r))^2. \tag{6.15}$$

The first sum equals

$$\begin{aligned}
&\sum_{\partial(a)=m} \left( \sum_{\substack{p|a \\ \partial(p)\le r}} f(p) \right)^2 \\
&= \sum_{\partial(p)\le r} f^2(p) \sum_{\substack{\partial(a)=m \\ p|a}} 1 + \sum_{\substack{p_1\ne p_2 \\ \partial(p_1)\le r, \partial(p_2)\le r}} f(p_1)f(p_2) \sum_{\substack{\partial(a)=m \\ p_1|a, p_2|a}} 1 \\
&= Aq^m \sum_{\partial(p)\le r} f^2(p)q^{-\partial(p)}\left(1+O(m^{-\gamma})\right) \\
&\quad + Aq^m \sum_{\substack{p_1\ne p_2 \\ \partial(p_1)\le r, \partial(p_2)\le r}} f(p_1)f(p_2)q^{-\partial(p_1)-\partial(p_2)}\left(1+O(m^{-\gamma})\right) \\
&= Aq^m \left[\sigma^2(r)\left(1+O(m^{-\gamma})\right) + \left((\bar{\mu}(r))^2 - \sum_{\partial(p)\le r} f^2(p)q^{-2\partial(p)}\right)\right. \\
&\quad \left. \times \left(1+O(m^{-\gamma})\right)\right].
\end{aligned}$$

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

The second sum in (6.15) equals

$$\begin{aligned}\sum_{\partial(a)=m}\ \sum_{\substack{p|a\\ \partial(p)\le r}} f(p) &= \sum_{\partial(p)\le r} f(p) \sum_{\substack{\partial(a)=m\\ p|a}} 1\\ &= Aq^m\bar{\mu}(r)\left(1+O(m^{-\gamma})\right).\end{aligned}$$

Note that, by the Cauchy–Schwarz inequality,

$$\begin{aligned}|\bar{\mu}(r)| &\le \left[\sum_{\partial(p)\le r} f^2(p)q^{-\partial(p)}\right]^{\frac{1}{2}}\left[\sum_{\partial(p)\le r} q^{-\partial(p)}\right]^{\frac{1}{2}}\\ &\ll \sigma(r)(\log r)^{\frac{1}{2}},\end{aligned}$$

and that

$$\sum_{\partial(p)\le r} f^2(p)q^{-2\partial(p)} = o\left(\sigma^2(r)\right).$$

Then (6.14) follows since $(\log r)^{\frac{1}{2}}m^{-\gamma}\to 0$.

Similarly we can prove (6.7). □

The next theorem specifies the normal distribution. We need one more lemma for its proof.

(7.6.3) LEMMA. *Let $\sigma(x)$ be a non–decreasing function, defined for $0<x<\infty$ and positive for sufficiently large $x$. Then there exists a function $r(x)$ such that*

$$\frac{r}{x}\longrightarrow 0,\quad \frac{\sigma(r)}{\sigma(x)}\longrightarrow 1 \tag{6.16}$$

*as $x\to\infty$ if and only if for each fixed positive number $\alpha$,*

$$\frac{\sigma(\alpha x)}{\sigma(x)}\longrightarrow 1 \tag{6.17}$$

*as $x\to\infty$.*

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

PROOF. First, assume that the two conditions in (6.16) hold. Note that $\sigma(x)$ is non-decreasing, and that if $0 < \alpha < 1$ then $r < \alpha x < x$ for $x$ sufficiently large. Hence

$$\frac{\sigma(r)}{\sigma(x)} \leq \frac{\sigma(\alpha x)}{\sigma(x)} \leq 1,$$

and (6.17) follows if $0 < \alpha \leq 1$. If $1 < \alpha$, then $0 < \frac{1}{\alpha} < 1$, and we have

$$\frac{\sigma(\alpha x)}{\sigma(x)} = \left(\frac{\sigma\left(\frac{1}{\alpha}(\alpha x)\right)}{\sigma(\alpha x)}\right)^{-1} \to 1$$

as $x \to \infty$.

Then assume (6.17). Then, for each $k \in \mathbb{N}$, there exists $x_k$ such that

$$\left|\frac{\sigma\left(\frac{1}{k}x\right)}{\sigma(x)} - 1\right| \leq \frac{1}{k},$$

for all $x \geq x_k$. We may assume that $0 < x_1 < x_2 < \cdots$, and $x_k \to \infty$ as $k \to \infty$. Let $y_0 = 0$ and $y_k = x_k + x_{k+1}$, $k \geq 1$. Define

$$r(x) = \frac{y_k}{k}\,\frac{y_{k+1} - x}{y_{k+1} - y_k} + \frac{y_{k+1}}{k+1}\,\frac{x - y_k}{y_{k+1} - y_k},$$

for $y_k \leq x < y_{k+1}$, $k = 0, 1, 2, \ldots$. Then $r(x)$ is continuous. We have

$$r(x) \leq \frac{1}{k}\left(y_k \frac{y_{k+1} - x}{y_{k+1} - y_k} + y_{k+1}\frac{x - y_k}{y_{k+1} - y_k}\right) = \frac{x}{k}$$

and, similarly,

$$r(x) \geq \frac{x}{k+1}$$

for $y_k \leq x < y_{k+1}$. Hence

$$\frac{1}{k+1} \leq \frac{r(x)}{x} \leq \frac{1}{k},$$

and

$$\frac{\sigma\left(\frac{1}{k+1}x\right)}{\sigma(x)} \le \frac{\sigma(r)}{\sigma(x)} \le 1$$

for $y_k \le x < y_{k+1}$. Note that $x > x_{k+1}$ when $x \ge y_k$. Hence

$$1 - \frac{1}{k+1} < \frac{\sigma(r)}{\sigma(x)} \le 1$$

for $y_k \le x < y_{k+1}$. This proves (6.16). □

(7.6.4) THEOREM. (cf. Zhang [3]) *Suppose that (6.3) holds with $A > 0$, $q > 1$, and $c \ge 0$. Let $f$ be a real-valued strongly additive function on $\mathcal{G}$. In order that*

$$\frac{1}{G(m)}\nu_m\left(f(a) - \bar{\mu}(m) \le x\sigma(m)\right) \to \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}dt \tag{6.18}$$

*uniformly as $m \to \infty$ it is sufficient that*

$$\frac{1}{\sigma^2(m)} \sum_{\substack{\partial(p)\le m \\ |f(p)|\ge\varepsilon\sigma(m)}} f^2(p)q^{-\partial(p)} \to 0 \tag{6.19}$$

*as $m \to \infty$, for each fixed $\varepsilon > 0$.*

*Conversely, if $f$ belongs to the class $H$ then the condition (6.19) is also necessary.*

*Remark.* Condition (6.19) is an analogue of the well-known *Lindeberg condition* in probability theory (cf. Billingsley [1]).

PROOF. If (6.19) holds for each fixed $\varepsilon > 0$, then, for $0 < \alpha < 1$,

$$1 - \frac{\sigma^2(\alpha m)}{\sigma^2(m)} = \frac{1}{\sigma^2(m)} \sum_{\substack{\alpha m<\partial(p)\le m \\ |f(p)|\le\varepsilon\sigma(m)}} f^2(p)q^{-\partial(p)}$$

$$+\frac{1}{\sigma^2(m)} \sum_{\substack{\alpha m<\partial(p)\leq m \\ |f(p)|>\varepsilon\sigma(m)}} f^2(p)q^{-\partial(p)}$$
$$\leq \varepsilon^2 \sum_{\alpha m<\partial(p)\leq m} q^{-\partial(p)} + o_\varepsilon(1).$$

The last sum equals

$$\sum_{\alpha m<n\leq m} q^{-n}P(n) = \log\frac{1}{\alpha} + O\left((\alpha m)^{-1}\right),$$

by (3.4) of Chapter 3. Therefore

$$\limsup_{m\to\infty}\left(1-\frac{\sigma^2(\alpha m)}{\sigma^2(m)}\right) \leq \varepsilon^2\log\frac{1}{\alpha}.$$

Letting $\varepsilon \to 0$, we obtain,

$$\lim_{m\to\infty}\left(1-\frac{\sigma^2(\alpha m)}{\sigma^2(m)}\right) = 0,$$

and hence (6.17) follows. Thus, by Lemma 7.6.3, $f$ must be of class $H$. Also, (6.19) implies that

$$\frac{1}{\sigma^2(m)} \sum_{\substack{\partial(p)\leq m \\ f(p)\leq-\varepsilon\sigma(m)}} f^2(p)q^{-\partial(p)} \to 0,$$

and

$$\frac{1}{\sigma^2(m)} \sum_{\substack{\partial(p)\leq m \\ f(p)\leq\varepsilon\sigma(m)}} f^2(p)q^{-\partial(p)}$$
$$= \frac{1}{\sigma^2(m)}\left(\sigma^2(m) - \sum_{\substack{\partial(p)\leq m \\ f(p)>\varepsilon\sigma(m)}} f^2(p)q^{-\partial(p)}\right) \to 1$$

as $m \to \infty$, for each $\varepsilon > 0$. Hence (6.5) holds with the distribution function

$$K(x) = \begin{cases} 1, & \text{if } x \geq 0, \\ 0, & \text{if } x < 0. \end{cases} \tag{6.20}$$

Since the limit distribution has characteristic function

$$\begin{aligned}\phi(t) &= \exp\left\{\int_{-\infty}^{\infty}\left(e^{itx}-1-itx\right)x^{-2}dK(x)\right\} \\ &= e^{-t^2/2},\end{aligned}$$

the limit distribution is the standard normal. Thus (6.18) follows from Theorem 7.6.1.

Conversely, if $f(a)$ is of class $H$, then (6.19) follows from (6.18), (6.6), and (6.5). □

The following theorem (Zhang [3]) is an immediate consequence of Theorem 7.6.4.

(7.6.5) THEOREM. *Suppose that (6.3) holds with $A > 0$, $q > 1$, and $c \geq 0$. Let $f$ be a real-valued strongly additive function on $\mathcal{G}$ such that $|f(p)| \leq 1$ for all primes $p$, and such that $\sigma(m) \to \infty$ as $m \to \infty$. Then*

$$\frac{1}{G(m)}\nu_m\left(f(a)-\bar{\mu}(m) \leq x\sigma(m)\right) \to \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}dt$$

*uniformly as $m \to \infty$.*

Actually, in the case of Theorem 7.6.5, $\varepsilon\sigma(m) \to \infty$ as $m \to \infty$ for each fixed $\varepsilon > 0$, and hence

$$\sum_{\substack{\partial(p)\leq m \\ |f(p)|\geq\varepsilon\sigma(m)}} f^2(p)q^{-\partial(p)} = 0$$

for $m$ sufficiently large.

As an interesting application of Theorem 7.6.5, we consider the function given by $f(a) = \omega(a)$, the total number of distinct prime divisors of $a$. This was investigated earlier in Theorem 3.3.6 and (especially) in Theorem 3.3.7, an analogue of the Hardy–Ramanujan theorem. Now, by (3.4) of Chapter 3,

$$\bar{\mu}(m) = \sigma^2(m) = \sum_{\partial(p) \leq m} q^{-\partial(p)} = \log m + c + O(m^{-1}).$$

Since $|f(p)| = 1$, Theorem 7.6.5 implies that

$$\frac{1}{G(m)} \nu_m \left( \frac{\omega(a) - \log m}{\sqrt{\log m}} \leq x \right) \to \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{x} e^{-t^2/2} dt$$

uniformly as $m \to \infty$, which is an analogue of the celebrated result of Erdős and Kac [1,2].

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

## 7.7 Rate of Convergence to the Normal Law

To conclude our discussion on this chapter, we state, without proof, a central limit theorem with a best possible error estimate for additive functions as well as for strongly additive functions on arithmetical semigroups (cf. Zhang [5]).

Let $f$ be a real–valued additive function defined on an arithmetical semigroup $\mathcal{G}$. Let $\beta(m)$ be an arithmetic function defined for $m \in \mathbb{N}$, such that $\beta(m) \to \infty$ as $m \to \infty$. Also let

$$\alpha(m) := \sum_{\substack{k\partial(p)\leq m \\ \left|f\left(p^k\right)\right|\leq\beta(m)}} f(p^k)q^{-k\partial(p)}\left(1 - q^{-\partial(p)}\right), \tag{7.1}$$

and

$$\Phi(x) = \frac{1}{\sqrt{2\pi}}\int_{-\infty}^{x} e^{-t^2/2}dt.$$

(7.7.1) THEOREM. *Assume that*

$$G(m) = Aq^m + O\left(q^m m^{-\gamma}\right), \quad m \geq 1 \tag{7.2}$$

*holds with constants* $A > 0$, $q > 1$, *and* $\gamma > 2$. *Then the estimate*

$$\frac{1}{G(m)}\nu_m\left(f(a) - \alpha(m) \leq x\beta(m)\right) = \Phi(x) + O\left(\inf_{\varepsilon>0}\Delta(\varepsilon; m)\right), \tag{7.3}$$

*with*

$$\begin{aligned}\Delta(\varepsilon; m) : \ = \ & \varepsilon + \sum_{\substack{\partial(p)\leq m \\ |f(p)|>\varepsilon\beta(m)}} q^{-\partial(p)} + \left|1 - \frac{1}{\beta^2(m)}\sum_{\substack{\partial(p)\leq m \\ |f(p)|\leq\varepsilon\beta(m)}} f^2(p)q^{-\partial(p)}\right| \\ & + \frac{1}{\beta^2(m)}\sum_{\substack{k\partial(p)\leq m,\, k\geq 2 \\ \varepsilon\beta(m)<\left|f\left(p^k\right)\right|\leq\beta(m)}} f^2(p^k)q^{-k\partial(p)}\end{aligned}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

$$+ \sum_{\substack{k\partial(p)\leq m,\, k\geq 2 \\ \left|f\left(p^k\right)\right|>\beta(m)}} q^{-k\partial(p)} + \sum_{\substack{k\partial(p)\leq \frac{\log 2}{\log q},\, k\geq 2 \\ \varepsilon\beta(m)<\left|f\left(p^k\right)\right|\leq\beta(m)}} q^{-k\partial(p)} \tag{7.4}$$

*holds uniformly for all real $x$, and $m \geq \frac{\log 2}{2\log q}$. The $O$–constant in (7.3) depends as most on $A$, $q$, $\gamma$ and the $O$–constant in (7.2).*

In particular, if $f = \omega$ again, and,

$$\beta^2(m) = \sigma^2(m) = \log m + c + O(m^{-1}),$$

then, by Theorem 7.7.1, it can be shown that

$$\frac{1}{G(m)}\nu_m\left(\frac{\omega(a) - \log m}{\sqrt{\log m}} \leq x\right) = \Phi(x) + O\left((\log m)^{-\frac{1}{2}}\right),$$

where the error estimate is best possible (cf. Zhang [5]).

The counterpart of Theorem 7.7.1 in classical probabilistic number theory has a long history. Readers with interest in this history may read Elliott [1], Chapter 20, concluding remarks.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

# CHAPTER 8

# SURVEY OF SOME FURTHER TOPICS

## 8.1 Asymptotics of Factorizations

Commencing over 70 years ago, certain asymptotic problems were investigated by A. Oppenheim [1] and others, concerning "factorisatio numerorum" of integers, i.e. concerning especially (i) the total number $f(n)$ of factorizations of a natural number $n > 1$ into products of natural numbers larger than 1, when the order of the factors is *disregarded*, and (ii) the corresponding total number $F(n)$ of factorizations when the order of the factors is *counted.* For instance, $f(12) = 4$ while $F(12) = 8$.

It is meaningful to consider such questions also within the partly analogous but distinct context of additive arithmetical semigroup $\mathcal{G}$. The following two basic results were obtained by A. Knopfmacher, et al. [1]:

(8.1.1) THEOREM. *If $\mathcal{G}$ satisfies Axiom $\mathcal{A}^{\#}$, then the average number of unordered factorizations of an element of degree n in $\mathcal{G}$ has the form*

$$\bar{f}(n) = C_{\mathcal{G}} n^{-3/4} \exp\left(2\sqrt{An}\right)\left(1 + O\left(n^{-\frac{1}{2}}\right)\right) \quad \textit{as} \quad n \to \infty,$$

*where*

$$C_{\mathcal{G}} = \frac{A^{-3/4}e^{A/2}}{2\sqrt{\pi}} \exp\left(\sum_{m=0}^{\infty}\left(G(m) - Aq^{m}\right)q^{-m} + \sum_{k=2}^{\infty}\frac{Z(q^{-k}) - 1}{k}\right).$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

The asymptotic estimation of *ordered* factorizations is far simpler than that in Theorem 8.1.1, which appears to require more delicate techniques of complex contour integration. The conclusion for the ordered case (under a weaker hypothesis than Axiom $\mathcal{A}^{\#}$) is given by:

(8.1.2) THEOREM. *Suppose that $\mathcal{G} \neq \{1\}$ has zeta function $Z(y)$ which is holomorphic in some disc $|y| < r$, and takes values larger than 2 for some real values of $y < r$. Then*

$$\bar{F}(n) = \frac{y_0^{-n-1}}{Z'(y_0)} + O\left(t_0^{-n}\right) \quad \textit{as} \quad n \to \infty,$$

*where $y_0 \in (0, r)$ is the unique real solution of $Z(y) - 2 = 0$, and $y_0 < t_0 < r$.*

A more subtle version of this theorem, requiring a more delicate proof, is given by A. Knopfmacher, et al. [2]:

Suppose that $\mathcal{G}$ has an infinite subset $E$ of elements $\neq 1$, whose "zeta" function

$$Z_E(y) = 1 + \sum_{n=1}^{\infty} E(n) y^n$$

is holomorphic in some disc $|y| < r$, where $E(n) = \#\{e \in E : \partial(e) = n\}$. Also suppose that $\lim_{\text{real } y \to r^{-1}} Z_E(y) > 2$, and that there exist positive integers $k_1, \ldots, k_h$ with g.c.d. one, such that $E(k_i) > 0$. Then let $F_E(b)$ equal the total number of ordered factorizations of $b \in \mathcal{G}$ into elements of $E$.

(8.1.3) THEOREM. *Under the preceding assumptions on $E$,*

$$\bar{F}_E(n) = \sum_{\partial(b)=n} F_E(b) = \frac{y_0^{-n-1}}{Z_E'(y_0)} + O\left(t_0^{-n}\right) \quad \textit{as} \quad n \to \infty,$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

*where $y_0 \in (0, r)$ is the unique real solution of $Z_E(y) - 2 = 0$, and $y_0 < t_0 < r$.*

This result is the analogue of a sharpened form of a theorem of Erdős [1] for positive integers, also given by A. Knopfmacher, et al. [2]. The latter reference also determines the exact values of the constants which occur in Theorem 8.1.3, when $\mathcal{G}$ satisfies Axiom $\mathcal{A}^{\#}$, and $E$ is the set $\mathcal{P}$ of all *prime* elements in $\mathcal{G}$ or the set $\mathcal{G}_{(2)}$ of all *square-free* elements in $\mathcal{G}$.

After deriving estimates for the numbers of unordered and ordered factorizations of elements of $\mathcal{G}$, a natural sequel would be to investigate the *lengths* (i.e. the numbers of factors) of the unordered and ordered factorizations of elements of $\mathcal{G}$. The following results provide asymptotic estimates for the *means* and *variances* of these lengths for elements of degree $n$ in $\mathcal{G}$; see A. Knopfmacher, et al. [3].

(8.1.4) THEOREM. *Let $\mathcal{G}$ satisfy Axiom $\mathcal{A}^{\#}$. Then the mean $\mu(n)$ and variance $\nu(n)$ for the lengths of unordered factorizations of elements of degree $n$ in $\mathcal{G}$ have the form*

$$\mu(n) = \sqrt{An}(1 + \cdots), \quad \nu(n) = \frac{1}{2}\sqrt{An}(1 + \cdots),$$

*where in each case $\cdots$ indicates an asymptotic expansion in powers of $1/\sqrt{n}$.*

*Note:* The symbols $\mu$ and $\nu$ used here should not be confused with other uses of these symbols in the present book.

(8.1.5) THEOREM. *Suppose that $\mathcal{G} \neq \{1\}$ has a zeta function $Z(y)$ with positive radius of convergence $R$. Also suppose that $Y(\omega) := Z(\omega) - 1$ satisfies the conditions:*

*(i) $Y(\rho) = 1$ for some $\rho \in (0, R)$, and*

*(ii)* $Y(\omega) \neq 1$ *for all* $\omega \neq \rho$ *with* $|\omega| = \rho$.

*Then the mean* $\hat{\mu}(n)$ *and variance* $\hat{\nu}(n)$ *for the lengths of ordered factorizations of elements of degree* $n$ *in* $\mathcal{G}$ *satisfy*

$$\hat{\mu}(n) = an + b + O(n\theta^n), \quad \hat{\nu}(n) = cn + d + O(n^2\theta^n),$$

*where* $a, b, c, d$, *and* $\theta$ *with* $\theta \in (0, 1)$, *are constants depending on* $\mathcal{G}$, *which can be explicitly specified.*

Theorems about more general additive arithmetical semigroups *sometimes simplify considerably* for the important special semigroup $\mathcal{G}_q$ of all *monic polynomials in one indeterminate* over $\mathbb{F}_q$, but this is *not always* the case. For example, Theorem 8.1.5 simplifies as below (cf. A. Knopfmacher, et al. [3]), while the earlier theorems of this section *do not* appear to admit similar reductions.

(8.1.6) THEOREM. *For the semigroup* $\mathcal{G}_q$,

$$\hat{\mu}(n) = \begin{cases} 1, & \textit{if } n = 1, \\ \dfrac{n+1}{2}, & \textit{if } n > 1, \end{cases} \qquad \hat{\nu}(n) = \begin{cases} 1, & \textit{if } n = 1, \\ \dfrac{n-1}{4}, & \textit{if } n > 1. \end{cases}$$

The following different types of results about factorizations, due to A. Knopfmacher and Warlimont [1], exhibit some instances of asymptotic statements which are especially intuitive in the case of the special semigroup $\mathcal{G}_q$:

Many deterministic as well as probabilistic factorization algorithms for a polynomial in $\mathcal{G}_q$ require that a distinct–degree factorization of the polynomial be performed as the initial step; see e.g. Knuth [1]. In particular, the further application of all such algorithms becomes unnecessary if the polynomial has only irreducible factors of distinct degrees. It is therefore of interest to determine the probability of the last case, when such methods are being applied. For large $q \to \infty$, Greene and Knuth [1] showed that an asymptotic probability $e^{-\gamma}$ is obtained, where $\gamma$ is Euler's classical constant. However, such factorization algorithms are usually applied over small finite fields, and the following theorem applies over *any* fixed field $\mathbb{F}_q$.

(8.1.7) THEOREM. *Let $\gamma_0(n,q)$ denote the number of polynomials $f$ of degree $n$ in $\mathcal{G}_q$ of the form $f = p_1 p_2 \cdots p_k$ for some irreducible polynomials $p_1, \ldots, p_k$ of distinct degrees. Also let $\gamma_1(n,q)$ denote the number of polynomials $f$ of degree $n$ in $\mathcal{G}_q$ of the form $f = p_1^{r_1} p_2^{r_2} \cdots p_k^{r_k}$ for some irreducible polynomials $p_1, \ldots, p_k$ of distinct degrees, and some exponents $r_1, \ldots, r_k$. Then there exists a constant $c > 0$ such that for $j = 0, 1$*

$$\left|\gamma_j(n,q)q^{-n} - L_j(q)\right| < \frac{c}{n},$$

*where*

$$L_j(q) = \prod_{m=1}^{\infty} \left(1 + \frac{P_q(m)}{q^m - j}\right) e^{-1/m}.$$

The limiting constants

$$L_j(q) = \lim_{n\to\infty} \gamma_j(n,q)q^{-n}$$

are also computed and estimated accurately by A. Knopfmacher and Warlimont [1], showing in particular that for $q \geq 11$ they are already fairly close to the earlier asymptotic probability $e^{-\gamma} = 0.5614\ldots$.

Rather wide-ranging generalizations of Theorem 8.1.7 were obtained by A. Knopfmacher and Warlimont [2] for an arbitrary (additive) arithmetical semigroup $\mathcal{G}$ satisfying the hypothesis

$$\sum_{n=0}^{\infty} \sup_{m\geq n} \left|G(m)q^{-m} - A\right| < \infty,$$

which occurred for example in Theorem 3.2.1 and 3.3.1 earlier. For more details, we refer to the paper just cited, which deals also with still more general factorization patterns than those involved for $\gamma_j(n,q)$ above. Recently, R. Warlimont has obtained various extra results (as yet unpublished) which sharpen or extend the preceding conclusions further; for still further results, see also A. Knopfmacher and Ridley [1], and A. Knopfmacher and Warlimont [3].

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

## 8.2 Direct Factors of Arithmetical Semigroups

Earlier in this book we have occasionally considered the question of determining the existence and value of the asymptotic density

$$\delta(E) = \lim_{n\to\infty} \frac{E(n)}{G(n)}$$

of a specific subset $E$ of $\mathcal{G}$. An interesting case in which this is always possible occurs when $E$ is an algebraic **direct factor** of $\mathcal{G}$, i.e. when there exists a subset $F$ of $\mathcal{G}$ such that every element $a \in \mathcal{G}$ can be expressed uniquely in the form $a = ef$ for elements $e \in E$, $f \in F$. In such a case, we shall write $\mathcal{G} = E \otimes F$.

For example, for any fixed positive integer $k$, we have $\mathcal{G} = \mathcal{G}^k \otimes \mathcal{G}_{(k)}$ where $\mathcal{G}^k$ is the set of all $k$–th powers $a^k (a \in \mathcal{G})$, and $\mathcal{G}_{(k)}$ is the set of all *$k$-free* elements of $\mathcal{G}$. Also, if $\mathcal{P} = P \cup Q$ is a partition of the set $\mathcal{P}$ of all prime elements of $\mathcal{G}$ into disjoint subsets $P$, $Q$, and $E_R$ denotes the sub–semigroup generated in $\mathcal{G}$ by a subset $R$ of $\mathcal{P}$, then $\mathcal{G} = E_P \otimes E_Q$.

By way of illustration, we note that the results described below include the earlier Propositions 1.3.8 and 1.1.9 (which covered the preceding examples for any $k \geq 1$, and any finite subset $P$ of $\mathcal{P}$). The general results, which are due to Indlekofer, J. Knopfmacher and Warlimont [1], are analogues of theorems for the semigroup of $\mathbb{N}$ of all natural numbers, due to Saffari [1] and Erdős, et al. [1]. The case of the special semigroup $\mathcal{G}_q$ was partially treated by J. Knopfmacher [1].

(8.2.1) THEOREM. *Suppose that $\mathcal{G} = E \otimes F$, and let $Z_H(y) = \sum_{n=0}^{\infty} H(n)y^n$ denote the "zeta" function of a subset $H$ of $\mathcal{G}$, formally putting $H(0) = 1$ even if $1 \notin H$.*

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

(i) *If $G(n) \sim Aq^n$ as $n \to \infty$, for constants $A > 0$, $q > 1$ then $E$ and $F$ have asymptotic densities $\delta(E)$, $\delta(F)$ and $\delta(E) = Z_F(q^{-1})^{-1}$, $\delta(F) = Z_E(q^{-1})^{-1}$, where $Z_H(q^{-1})^{-1} = 0$ if $Z_H(q^{-1}) = \infty$.*

(ii) *If $\mathcal{G}$ satisfies Axiom $\mathcal{A}^{\#}$, then $Z_{E\cap\mathcal{P}}(q^{-1}) < \infty$ implies $Z_E(q^{-1}) < \infty$. If further $E \cap \mathcal{P} = \emptyset$, then $\sum_{e\in E} t^{\sqrt{\partial(e)}} q^{-\partial(e)} < \infty$ for $1 \leq t < q$.*

A special type of direct factor $E$ has been investigated in more detail by Warlimont [6] under Axiom $\mathcal{A}^{\#}$:

Given some integer $k > 1$, let $\mathcal{R}$ denote the union of $h$ $(< \varphi(k))$ distinct residue classes $\mathcal{R}_1, \ldots, \mathcal{R}_h$ of integers, where $\mathcal{R}_j$ is the class of integers $m \equiv r_j \pmod{k}$ for an integer $r_j$ coprime to $k$. Then let $E = E(\mathcal{R})$ denote the set of all elements of $\mathcal{G}$ whose prime factors $p$ all have $\partial(p) \in \mathcal{R}$. In that case, $E(\mathcal{R})$ coincides with the earlier example $E_R$ of a direct factor, with $R = \{p \in \mathcal{P} : \partial(p) \in \mathcal{R}\}$. Warlimont [6] studies the asymptotic approach of $E_R(n)/G(n)$ to its limit $\delta(E_R)$ in a subtle way, according to properties of $k$ and the zeta function of $\mathcal{G}$. In particular, his main conclusion is:

(8.2.2) THEOREM. *If $k$ is odd, then*

$$E_R(n) \sim KG(n)n^{-1+h/k} \quad \textit{as} \quad n \to \infty$$

*through multiples of $d := \gcd(r_1, \ldots, r_h, k)$, for a constant $K > 0$ depending on $\mathcal{R}$ and $\mathcal{G}$.*

Interested readers may wish to consult Warlimont [6] for corresponding information about situations in which $k$ is *even.*

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

## 8.3 Sets of Multiples

Previously in this book we have considered only one type of asymptotic density $\delta(E)$ when relevant, for a subset $E$ of $\mathcal{G}$. In classical analytic number theory, variations of ordinary asymptotic density are sometimes significant in the study of subsets of the natural numbers $\mathbb{N}$. In parallel with this, Warlimont [5] studied variations of $\delta(E)$ in proving analogues for $\mathcal{G}$ of some basic theorems on "sets of multiples" in $\mathbb{N}$ (which were included recently in the book by Hall [1], for example).

Given $B \subseteq \mathcal{G}$, consider then the set $M(B)$ of all elements $a \in \mathcal{G}$ which are multiples in $\mathcal{G}$ of at least one element $b \in B$. In order to investigate the asymptotic density of $M(B)$, Warlimont [5] first considers (with slightly different notations) the following variations of this concept for a subset $H$ of $\mathcal{G}$:

Letting $H(n) = \#\{a \in H : \partial(a) = n\}$ as before, define

$$\begin{aligned}
\underline{\delta}(H) &= \underline{\lim}_{n\to\infty} \frac{H(n)}{G(n)}, \quad \overline{\delta}(H) = \overline{\lim}_{n\to\infty} \frac{H(n)}{G(n)}, \\
\underline{\delta}_0(H) &= \underline{\lim}_{n\to\infty} \frac{1}{n+1} \sum_{m=0}^{n} \frac{H(m)}{G(m)}, \\
\overline{\delta}_0(H) &= \overline{\lim}_{n\to\infty} \frac{1}{n+1} \sum_{m=0}^{n} \frac{H(m)}{G(m)},
\end{aligned}$$

and let

$$\delta(H) = \lim_{n\to\infty} \frac{H(n)}{G(n)}, \quad \delta_0(H) = \lim_{n\to\infty} \frac{1}{n+1} \sum_{m=0}^{n} \frac{H(m)}{G(m)},$$

if the limits exist. Then $\delta_0$ is a kind of parallel to "*logarithmic density*" in $\mathbb{N}$, and

$$\underline{\delta}(H) \le \underline{\delta}_0(H) \le \overline{\delta}_0(H) \le \overline{\delta}(H).$$

Thus $\delta_0(H)$ exists and equals $\delta(H)$, if $\delta(H)$ exists. The converse is *not* necessarily true; see Theorem 8.3.2 (ii) below.

The results below were all derived by Warlimont [5]: First suppose that there are constants $A > 0$, $q > 1$ such that

$$G(n) \sim Aq^n \quad \text{as} \quad n \to \infty.$$

Then, by using the "principle of inclusion and exclusion" or "sieve formula" of combinatorics, Warlimont shows that $\delta(M(E))$ exists for every *finite* subset $E$ of $\mathcal{G}$, and if $E = \{e_1, \ldots, e_k\}$ then

$$\delta(M(E)) = \sum_{r=1}^{k}(-1)^{r+1} \sum_{1\leq j_1<\cdots<j_r\leq k} q^{-\partial\left(l.c.m.(e_{j1},\ldots,e_{jr})\right)}.$$

Hence

$$\delta^*(M(B)) := \sup\{\delta(M(E)) : \ E \subseteq B, \ E \text{ finite }\}$$

is always well-defined, and $\delta^*(M(B)) \leq \underline{\delta}(M(B))$.

(8.3.1) THEOREM. *Suppose that $G(n) \sim Aq^n$ as $n \to \infty$, for constants $A > 0$, $q > 1$. Let $B$ be any subset of $\mathcal{G}$ such that $\sum_{b\in B} q^{-\partial(b)} < \infty$, or the elements of $B$ are pairwise coprime. Then $\delta(M(B))$ exists, with value $\delta(M(B)) = \delta^*(M(B))$.*

The next theorem of Warlimont is based on longer and more delicate arguments:

(8.3.2) THEOREM. *Suppose that $\mathcal{G}$ satisfies Axiom $\mathcal{A}^{\#}$. Then $\delta_0(M(B))$ exists for every subset $B$ of $\mathcal{G}$, and*

$$\delta_0(M(B)) = \delta^*(M(B)) = \underline{\delta}(M(B)).$$

*(ii) Given any $\varepsilon > 0$, there exists a subset $B_\varepsilon$ of $\mathcal{G}$ such that $\underline{\delta}(M(B_\varepsilon)) < \varepsilon$, while $\overline{\delta}(M(B_\varepsilon)) = 1$.*

These results are analogues of two theorems for ℕ due to Davenport and Erdős, and Besicovich, respectively. They appear to be precursors of

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

various other interesting analogues of results relating to classical sets of multiples in ℕ, which the first named author of the present book hopes to treat elsewhere.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

## 8.4 Further Properties of Special Sets and Functions

In Section 4.1 earlier, some properties of the prime divisor functions $\omega$ and $\Omega$ were studied within the so-called "classical" case of Axiom $\mathcal{A}^{\#}$. Warlimont [7] has derived some further results as below, for the general case of Axiom $\mathcal{A}^{\#}$:

For integers $k$, $N \in \mathbb{N}$, first rewrite the earlier-defined functions $\pi_k(N)$, $\rho_k(N)$ and $\tau_k(N)$ as $\pi_1(N,k)$, $\pi_2(N,k)$ and $\pi_3(N,k)$, respectively.

Let $L(N,k) = \frac{(\log N)^{k-1}}{(k-1)!}$. Then, for the "classical" case of Axiom $\mathcal{A}^{\#}$ (here called *case* 1), Theorem 4.1.4 earlier has the corollary

$$\pi_j(N,k) = \frac{q^N}{N} L(N,k)(1+o(1)) \quad \text{as} \quad N \to \infty, \tag{4.1}$$

for fixed $k$. For the complementary *case* 2 of Axiom $\mathcal{A}^{\#}$ in which case 1 is false, Warlimont [7] adds firstly the conclusion

$$\pi_j(N,k) = \frac{q^N}{N} L(N,k)\left(1+(-1)^{N+k}+o(1)\right) \quad \text{as} \quad N \to \infty, \tag{4.2}$$

for fixed $k$. He then uses analogues of some classical number-theoretical techniques of A. Selberg in order to investigate the more difficult cases when $k$ may *vary* together with $N$. His main conclusion is:

(8.4.1) THEOREM. *Suppose that $\mathcal{G}$ satisfies Axiom $\mathcal{A}^{\#}$, and let $\Delta = \min\{\partial(p) : p \in \mathcal{P}\}$. Fix any real number $K > 0$ when $j = 1$ or 2, and fix some $K > 0$ with $K < q^{\Delta}$ when $j = 3$.*

*(i) In case 1 of Axiom $\mathcal{A}^{\#}$,*

$$\pi_j(N,k) = \frac{q^N}{N} L(N,k)\left\{F_j\left(\frac{k-1}{\log N}\right) + O_K\left(\frac{1}{\log N}\right)\right\}$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

*uniformly for* $1 \leq k \leq K \log N$.

(ii) *In case 2 of Axiom* $\mathcal{A}^{\#}$,

$$\pi_j(N,k) = \frac{q^N}{N} L(2N,k) \left\{ F_j \left( \frac{k-1}{\log 2N}, N+k \right) + O_K \left( \frac{1}{\log N} \right) \right\}$$

*uniformly for* $1 \leq k \leq K \log N$.

*Here* $F_j(z)$ *and* $F_j(z,h)$ *are explicitly definable functions of complex* $z$ *(and of* $h \in \mathbb{N}$ *in the second case).*

Some different problems concerning the prime divisors of elements of $\mathcal{G}$ concern asymptotic estimates for the numbers of elements of degree $n$ in $\mathcal{G}$, which are *free of* (or else are *divisible only by*) "large" prime elements $p$, i.e. primes $p$ with $\partial(p) > m$ (or $\partial(p) \leq m$, *respectively*). In other words, asymptotic estimates are sought for the functions

$$\psi(n,m) = \# \left\{ a \in \mathcal{G} : \ \partial(a) = n \text{ and } p|a \Rightarrow \partial(p) \leq m \right\},$$

and

$$\varphi(n,m) = \# \left\{ a \in \mathcal{G} : \ \partial(a) = n \text{ and } p|a \Rightarrow \partial(p) > m \right\}.$$

Such questions are analogous to well known ones of classical analytic number theory. Warlimont [5, Part 1] and Manstavicius [1,2] derived asymptotic estimates under Axiom $\mathcal{A}^{\#}$ for the functions $\psi(n,m)$ and $\varphi(n,m)$ as $n$, $m \to \infty$, and their conclusions involve delicate analogies with classical ones for natural numbers due to K. Dickman and A. Buchstab, as well as later authors. As with Theorem 8.4.1 above, the proofs and exact details are non–trivial and here we shall quote only two basic theorems of Warlimont [5]. Interested readers are referred to this paper for more details, as well as to Manstavicius [1,2] for very sharp further information. (The special semigroup $\mathcal{G}_q$ was also considered in a similar context by Car [1].)

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

(8.4.2) THEOREM. *Suppose that $\mathcal{G}$ satisfies Axiom $\mathcal{A}^{\#}$. Then*

$$\psi\left([m^u], m\right) \sim \rho(u) G\left([m^u]\right) \quad \textit{as} \quad m \to \infty,$$

*where $\rho(u)$ is the classical Dickman function of real $u \geq 0$.*

(8.4.3) THEOREM. *Suppose that $\mathcal{G}$ satisfies Axiom $\mathcal{A}^{\#}$.*

*(i) Then, in the "classical" case 1,*

$$\varphi\left([m^u], m\right) = e^{\gamma} \omega(u) W(m) G\left([m^u]\right) \quad \textit{as} \quad m \to \infty,$$

*where $\gamma$ is Euler's classical constant, $\omega(u)$ is Buchstab's classical function of real $u \geq 1$, and $W(m) = \prod_{\partial(p) \leq m} \left(1 - q^{\partial(p)}\right)$.*

*(ii) In case 2 of Axiom $\mathcal{A}^{\#}$,*

$$\varphi(n, m) = W(m) G(n) \left\{ e^{\gamma} \omega_j \left(\frac{n}{m}\right) + O\left(\frac{1}{m}\right) \right\}$$

*for $1 \leq m < n$, and $n \equiv j \,(\operatorname{mod} 2)$, where $e^{\gamma}\omega_0$ and $e^{\gamma}\omega_1$ are the fundamental functions $f$ and $F$, respectively, which occur in the classical "linear sieve" (cf. Halberstam and Richert [1], Chap. 8).*

*Remark.* In the proof of Theorem 8.4.3, Warlimont [5] derives and uses the following *Mertens type formula* subject to Axiom $\mathcal{A}^{\#}$:

$$W(m) := \prod_{\partial(p) \leq m} \left(1 - q^{-\partial(p)}\right) = \frac{e^{-\gamma}}{m} \left(1 + O\left(\frac{1}{m}\right)\right); \qquad (4.3)$$

cf. also Theorem 3.3.4 earlier.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

## 8.5 More About Polynomials and Finite Fields

It was stressed earlier that the multiplicative semigroup $\mathcal{G}_q$ of all *monic polynomials in one indeterminate* over a finite field $\mathbb{F}_q$ is one of the most basic and yet still interesting natural examples of an additive arithmetical semigroup satisfying Axiom $\mathcal{A}^{\#}$. A large proportion of the results treated in this book have corollaries for $\mathcal{G}_q$, which are *easy to read off* but still *non–trivial.* Since their proofs are usually no harder to develop within the abstract context of Axiom $\mathcal{A}^{\#}$, or sometimes even weaker assumptions, and since Axiom $\mathcal{A}^{\#}$ covers many other natural semigroups also, most of this book's preceding developments were carried out within a more abstract context, and without continual explicit singling out of the important special example $\mathcal{G}_q$.

In view of these remarks and because the other concrete examples described in Chapter 1 are also constructions founded essentially on finite fields, it is therefore indeed appropriate to regard the present book as being about a systematic branch of *"number theory arising from finite fields"*, despite the more abstract formulation of much of the discussion.

In making these remarks, *we emphasize* that there are certainly other topics which could be viewed as falling under a similar umbrella heading, e.g. further topics stemming also from algebraic geometry, or from non–archimedean analysis. Various such undoubtedly valid and significant *different* directions have been extensively treated by other authors, but they will not be pursued here; e.g. one should note the recent book by Goss [1], as well as its references.

Instead, we do wish to add a few more observations about some arithmetical properties of the important special semigroup $\mathcal{G}_q$ which are particularly *close in spirit* to the type of results developed in this book. Because of

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

its explicit concrete description, certain questions of analytic number theory for additive arithmetical semigroups have particularly simple answers for $\mathcal{G}_q$, in which asymptotic estimates can be replaced by exact algebraic formulae. Examples of this phenomenon occur if one compares certain of the asymptotic conclusions for arithmetical functions treated in Chapter 1 earlier with their algebraic counterparts for $\mathcal{G}_q$ as given in [AB], Chapter 3 – many of those conclusions going back to developments initiated by L. Carlitz around 65 years ago; e.g. see Carlitz [1,2,3], Carlitz and Cohen [1] and E. Cohen [1]. Nevertheless, as was noted e.g. in Section 8.1 above, *not all* phenomena or results of the analytic number theory of additive arithmetical semigroups have elementary or exact algebraic counterparts in the case of $\mathcal{G}_q$.

We conclude this section by describing a few more examples of theorems in the spirit of earlier results treated in this book, which admit particularly precise answers for the special semigroup $\mathcal{G}_q$, and also possess the novelty that certain of their proofs are *facilitated* by the *ad hoc* use of special new arithmetical semigroups; for further details, and references to work by others, see A. Knopfmacher and J. Knopfmacher [1,2]:

First let $M_q(n,k)$ denote the total number of polynomials of degree $n$ in $\mathcal{G}_q$ which have exactly $k \leq n$ *distinct* zeros in $\mathbb{F}_q$, and let $M_q^*(n,k)$ denote the corresponding number when $k$ counts the *multiplicity* of repeated zeros for a polynomial. Then explicit algebraic formulae can be derived for $M_q(n,k)$ and $M_q^*(n,k)$, for example

$$M_q(n,k) = \binom{q}{k} q^{n-k} \left(1 - \frac{1}{q}\right)^{q-k} \quad \text{if} \quad n \geq q, \tag{5.1}$$

and

$$M_q^*(n,k) = \binom{q+k-1}{k} q^{n-k} \left(1 - \frac{1}{q}\right)^{q} \quad \text{if} \quad n \geq q+k. \tag{5.2}$$

Such formulae can be used to deduce:

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

(8.5.1) THEOREM.

*(i) The mean or average number of distinct zeros in $\mathbb{F}_q$ of a polynomial of degree $n$ in $\mathcal{G}_q$ equals 1, and the variance about this average equals $1 - \frac{1}{q}$.*

*(ii) The mean or average number of zeros in $\mathbb{F}_q$ of a polynomial of degree $n$ in $\mathcal{G}_q$, when multiplicity of zeros is counted, equals*

$$\frac{q - q^{1-n}}{q-1} \to \frac{q}{q-1} \quad as \quad n \to \infty,$$

*while the corresponding variance about this average has the limit $\left(\frac{q}{q-1}\right)^2$ as $n \to \infty$.*

It is interesting to observe that (5.1) and (5.2) imply that the "probability" of obtaining $k$ zeros follows a *binomial probability* law with parameter $1/q$ for distinct zeros when $n \geq q$, and a truncated *negative binomial law* for $n \geq q + k$, when multiplicity of zeros is counted.

The preceding results can be extended considerably as below, with the added bonus of sharp applications to the prime divisor functions $\omega$ and $\Omega$ on $\mathcal{G}_q$:

Now let $M_q(n, k, r)$ denote the total number of polynomials of degree $n$ in $\mathcal{G}_q$ which have exactly $k \leq \min\left(\left[\frac{n}{r}\right], \pi(r)\right)$ *distinct* irreducible factors of degree $r$ in $\mathcal{G}_q$, where for brevity we *here write* $\pi(r) = P_q(r)$, and let $M_q^*(n, k, r)$ denote the corresponding number when *multiplicity* of repeated irreducible factors is counted; thus $M_q(n, k, 1) = M_q(n, k)$, $M_q^*(n, k, 1) = M_q^*(n, k)$. Exact algebraic formulae can be derived for these extended counting numbers, for example

$$M_q(n, k, r) = \binom{\pi(r)}{k} q^{n-kr} \left(1 - \frac{1}{q^r}\right)^{\pi(r)-k} \quad \text{if} \quad n \geq r\pi(r), \qquad (5.3)$$

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

and

$$M_q^*(n,k,r) = \binom{\pi(r)+k-1}{k} q^{n-kr}\left(1-\frac{1}{q^r}\right)^{\pi(r)} \quad \text{if} \quad n \geq r(\pi(r)+k). \tag{5.4}$$

Such formulae again lead to exact formulae for the *means*, as well as exact or asymptotic formulae for the corresponding *variances*, of the numbers of irreducible factors of degree $r$ of a polynomial of degree $n$ in $\mathcal{G}_q$, which are respectively distinct or counted with multiplicity. In more detail, we state:

(8.5.2) THEOREM.

*(i) The respective means are* $\pi(r)/q^r$, *and*

$$\frac{\pi(r)}{q^r-1}\left(1-q^{-r\left[\frac{n}{r}\right]}\right) \to \frac{\pi(r)}{q^r-1} \quad \textit{as} \quad n \to \infty.$$

*(ii) The respective variances about the means are exactly*

$$\pi(r)(q^r-1)/q^{2r} \quad \textit{if} \quad n \geq 2r, \quad \textit{or} \quad \pi(r)(q^r-\pi(r))/q^{2r} \quad \textit{if} \quad n < 2r,$$

*in the distinct case, and asymptotically*

$$\frac{\pi(r)q^r}{(q^r-1)^2} \quad \textit{as} \quad n \to \infty$$

*in the other case.*

For general $r \geq 1$, we remark that the two types of "probability" of $k$ irreducible factors of degree $r$ again follow respectively a *binomial probability* law or a truncated *negative binomial* law, with parameter $1/q^r$ now.

Next consider again the prime divisor functions $\omega$ and $\Omega$. Theorem 3.3.6 earlier implies asymptotic estimates for both these functions, of the form

$\log n + c + O(1/n)$ as $n \to \infty$, where $c$ is an explicitly definable constant depending on the function and semigroup under consideration. For $\mathcal{G}_q$, these averages for polynomials of degree $n$ can also be written explicitly in the form

$$\sum_{r=1}^{n} \frac{\pi(r)}{q^r}, \quad \text{or} \quad \sum_{r=1}^{n} \frac{\pi(r)}{q^r - 1}\left(1 - q^{-r\left[\frac{n}{r}\right]}\right), \tag{5.5}$$

respectively, in view of Theorem 8.5.2; these formulae also lead to the preceding asymptotic estimates in the case of $\mathcal{G}_q$.

The corresponding variances about the means of $\omega$ and $\Omega$ for polynomials of degree $n$ can be expressed by similar though more cumbersome algebraic formulae, which can be used to deduce:

(8.5.3) THEOREM. *The variances of $\omega$ and $\Omega$ about their means, for polynomials of degree $n$ in $\mathcal{G}_q$, have the form*

$$\log n + c' + O\left(\frac{\log n}{n}\right) \quad \textit{as} \quad n \to \infty$$

*where $c'$ is an explicit constant depending on the function under consideration.*

Lastly, although it differs from the main kinds of investigation treated in this book, we mention very briefly another parallel between the analytic number theory of $\mathcal{G}_q$ and $\mathbb{N}$, which stems from the special property (shared by polynomials and integers) that greatest common divisors (g.c.d.'s) can be determined by the "quotient–remainder" *Euclidean algorithm.* (Of course, some other mathematical objects also share such a property, but this is not generally true for elements of all arithmetical semigroups.)

Various authors (see initially Heilbronn [1] and Dixon [1]) have used methods and results of classical analytic number theory to derive asymptotic formulae involving the average *length* (or number of repetitions) of the

Euclidean algorithm needed to reach the g.c.d. of a pair of natural numbers $a, b$. Alternatively, this may be regarded as the average length of the finite simple *continued fraction* of the ratio $a/b$. The well-known algebraic analogies between polynomials and integers then made it seem plausible that parallel asymptotic conclusions should hold in the case of polynomials over $\mathbb{F}_q$.

In fact, after development of some initial analogies of this kind, it turned out that, *unlike* the situation for integers, exact algebraic formulae could be derived by algebraic and combinatorial methods for the case of polynomials over $\mathbb{F}_q$. These formulae yielded simple asymptotic *corollaries* of the required kind, but *without the need for* delicate tools of analysis or analytic number theory. Interested readers may refer in particular to the papers of A. Knopfmacher and J. Knopfmacher [3], A. Knopfmacher [1], and Friesen and Hensley [1], for actual formulae and further details.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

## 8.6 Ramanujan Expansions of Arithmetical Functions

In contrast with the usual asymptotic and quasi–statistical or probabilistic type of investigations of arithmetical functions and densities (which make up such a large portion of both classical analytic number theory, and the type of theory treated in most of this book under the different setting of additive arithmetical semigroups), a very intriguing different kind of analysis of arithmetical functions was initiated just over 80 years ago by the amazing self–taught mathematician Sriniwasa Ramanujan. This work, which is sketched very briefly below, was started by Ramanujan [1] and was carried forward soon afterwards by G.H. Hardy [1], and then later by many further researchers. Excellent surveys with large bibliographies have been provided in recent years by Schwarz [1,2] and Mauclaire [1], while Schwarz and Spilker [1] have recently provided a comprehensive introduction to such topics, as well as many of the more standard types of questions of classical analytic number theory whose analogues have been explored in this book.

In the case of general arithmetical semigroups, some initial analogies with classical results on so–called *Ramanujan expansions*, were developed by J. Knopfmacher ([AB], Chapter 7, and [5]), J. Knopfmacher and Slattery [1] and Slattery [1].

The last two cited works contain the beginnings of a comprehensive theory within the Axiom $\mathcal{A}^{\#}$ context, for which still further results may be expected.

A very rapid sketch of the abovementioned topics follows. Firstly, a key example of the innovative paper by Ramanujan [1] concerns the classical sum of divisors function $\sigma$ on $\mathbb{N}$, such that $\sigma(n) = \sum_{d|n} d$. Ramanujan

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

showed that

$$\frac{\sigma(n)}{n} = \frac{\pi^2}{6}\sum_{r=1}^{\infty}\frac{c_r(n)}{r^2}, \tag{6.1}$$

where $c_r(n)$ is the special trigonometric sum

$$c_r(n) = \sum_{\substack{1\leq a\leq r\\ \gcd(a,r)=1}} e^{2\pi ian/r} = \sum_{d|\gcd(r,n)} \mu\left(\frac{r}{d}\right) d. \tag{6.2}$$

Ramanujan, and soon afterwards Hardy, use *ad hoc* methods to establish (6.1) and various other striking expansions of arithmetical function values in terms of the sums $c_r(n)$, which later became commonly referred to as *Ramanujan sums.*

Next, certain authors noted further that expansions like (6.1) for an arithmetical function $f$ on $\mathbb{N}$ (e.g. for $f(n) = \sigma(n)/n$) can often (though not always) be expressed in the form

$$f(n) = \sum_{r=1}^{\infty} a_r(f)c_r(n) \quad \text{for all} \quad n \geq 1,$$

where

$$a_r(f) = \frac{1}{\phi(r)}m(f\cdot c_r), \quad m(g) = \lim_{n\to\infty}\frac{1}{n}\sum_{r\leq n} g(r).$$

On the basis of a suitable asymptotic *orthogonality* property of the functions $c_1, c_2, c_3, \ldots$, "explanations" were then sought for the existence of such pointwise convergent *"Ramanujan expansions"* of suitable arithmetical functions $f$, in terms of concepts and results parallel with classical *harmonic analysis.* (The significance of paying special attention to explanations based on analogies with classical-style harmonic analysis was recently brought out dramatically when Hildebrand [1] gave a short algebraic proof that *every* arithmetical function $f$ has an expansion

$$f(n) = \sum_{r=1}^{\infty} b_r c_r(n), \tag{6.3}$$

in terms of coefficients $b_r$ which can be defined recursively in terms of $f$, but *without* any obvious natural parallel to Fourier–type coefficients.)

Basic results of the above type of theory of arithmetical function expansions are surveyed and treated in the earlier works listed above. Interesting new approaches towards conceptual explanations for the existence of Ramanujan expansions for both those cases which can be fitted under the umbrella of a classical–type harmonic analysis (e.g. for functions $f$ like the (6.1) example), and for *other* interesting natural examples (e.g. the *divisor* function $d$ on $\mathbb{N}$), have recently been developed by Lucht [1,2].

For arithmetical semigroups, certain results were first developed in general and for Axiom $\mathcal{A}$ in the references by J. Knopfmacher cited above, and then for Axiom $\mathcal{A}^{\#}$ in the paper by J. Knopfmacher and Slattery [1]. A very brief sketch follows for the last case:

Firstly, it is clear from the second equation of (6.2) above that a possible fruitful analogue of the Ramanujan sum $c_r(n)$ when $r, n$ are now elements of a general arithmetical semigroup $\mathcal{G}$ is provided by

$$\sum_{d|\gcd(r,n)} \mu\left(\frac{r}{d}\right)|d|$$

for general $\mathcal{G}$ with Möbius function $\mu$, or by

$$c_r(n) := \sum_{d|\gcd(r,n)} \mu\left(\frac{r}{d}\right) q^{\partial(d)}$$

for an *additive* arithmetical semigroup $\mathcal{G}$ (the case which we shall *assume* for the rest of this section). It can then be verified that the new sums are not only meaningful in the generalized situation but *actually do* have properties similar to those of the classical Ramanujan sums.

Although the periodicity derived from the connection with trigonometrical sums in the classical case has no meaning in the generalized context,

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

a near replacement is provided by the concept of *evenness*, which was observed and developed by E. Cohen [1,2,3,4] for both classical arithmetical functions and similar functions of isomorphism classes of finite abelian groups. For general additive $\mathcal{G}$ and $k \in \mathcal{G}$, an arithmetical function is called **even** $(\bmod k)$ if and only if

$$f(n) = f((k,n)) \quad \text{for every} \quad n \in \mathcal{G},$$

where $(k,n) = \gcd(k,n)$ in $\mathcal{G}$. Then $c_r$ has this property for $r|k$, and it can be shown that $\{c_r : \ r|k\}$ spans the complex vector space of all functions on $\mathcal{G}$ which are even $(\bmod k)$. Thus $\{c_r : \ r \in \mathcal{G}\}$ spans the vector space $\mathcal{E}$ of all **even** functions on $\mathcal{G}$ (i.e. functions which are even $(\bmod k)$ for some $k \in \mathcal{G}$).

In analogy with classical theories of almost periodic functions, one may then consider concepts of *almost evenness.* In particular, since even functions must be bounded, we define a function $f$ to be **uniformly almost even** on $\mathcal{G}$ if and only if $f$ lies in the closure of $\mathcal{E}$ relative to the *uniform norm* $\| \ \|_u$ such that

$$\|g\|_u = \sup_{a \in \mathcal{G}} |g(a)|.$$

Also, in analogy with *Besicovitch's* classical theories of "almost periodicity", we call $f$ **almost even (B)** if and only if $f$ lies in the closure of $\mathcal{E}$ relative to the seminorm $\| \ \|_1$ such that

$$\|g\|_1 = \limsup_{n \to \infty} \frac{1}{G(n)} \sum_{\partial(a)=n} |g(a)|.$$

For a function $f$ of one of these last types, it can be shown *subject to Axiom* $\mathcal{A}^{\#}$ that all the **Ramanujan coefficients**

$$a_r(f) = \frac{1}{\phi(r)} m(f \cdot c_r)$$

exist, where now $\phi(r) := c_r(r)$ is one particular counterpart to the classical Euler function on $\mathbb{N}$. In particular, if $\sum_{a \in \mathcal{G}} (\mu * f)(a) q^{-\partial(a)}$ is absolutely

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

convergent, then it can be proved that $f$ is almost even $(B)$ and

$$a_r(f) = \sum_{b \in \mathcal{G},\, r|b} (\mu * f)(b) q^{-\partial(b)}. \tag{6.4}$$

Given the existence of the coefficients, it then becomes interesting to seek conditions under which $f$ has a pointwise convergent **Ramanujan expansion**:

$$f(n) = \sum_{r=1}^{\infty} a_r(f) c_r(n) \quad \text{for all} \quad n \in \mathcal{G}.$$

A number of further technical conditions on functions $f$ on $\mathcal{G}$ subject to Axiom $\mathcal{A}^{\#}$, which ensure both that $f$ is almost even $(B)$ and that its Ramanujan expansion is pointwise everywhere absolutely convergent, are treated in the paper by J. Knopfmacher and Slattery [1]. A fuller treatment of uniformly almost even and of so-called *almost even* $(B^{\lambda})$ functions subject to Axiom $\mathcal{A}^{\#}$ appears in the thesis of Slattery [1]. Still further results apparently remain to be developed in these directions.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

## 8.7 Additive Arithmetical Formations

One of the earliest definitive theorems of classical analytic number theory was the famous *Dirichlet Theorem on Primes in Arithmetical Progressions*, to the effect that there exist infinitely many integer primes $p \equiv r (\operatorname{mod} m)$ whenever $m, r$ are coprime positive integers. This theorem was published in 1837, and despite later simplifications has apparently never been proved in *complete generality* without some use of methods and results of analysis. After the much later establishment of the classical Prime Number Theorem, it was refined into the *Prime Number Theorem for Arithmetical Progressions*, which in its simplest form states that

$$\pi_{m,r}(x) \sim \frac{x}{\phi(m) \log x} \quad \text{as} \quad x \to \infty,$$

where $\pi_{m,r}(x)$ is the number of positive integer primes $p \leq x$ with $p \equiv r (\operatorname{mod} m)$, and $\phi$ is the classical Euler totient function.

This type of asymptotic *equidistribution* conclusion for prime numbers was soon accompanied earlier in the 20th century by similar types of theorems due to *E. Landau*, concerning prime ideals in *ideal classes*, in classical algebraic number theory.

Theorems of the above kinds were subsequently generalized by various authors into a type of **relative** abstract analytic number theory based on generalized "arithmetical progressions" or "ideal classes" within certain structures which extend or enlarge the scope of the Axiom $\mathcal{A}$ treated in [AB]. An introduction to this type of theory, with fuller details and references to earlier work (e.g. by Forman and Shapiro [1], J. Knopfmacher [8,9], and Müller [1,2]) is given in [AB], Chapter 9. In the remainder of this section, we shall only recall a few of the basic concepts and results involved, as a prelude to briefly sketching an impressive analogous theory initiated by Halter-Koch and Warlimont [1] for a context extending or enlarging the scope of Axiom $\mathcal{A}^{\#}$ for additive arithmetical semigroups.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Firstly consider an arbitrary arithmetical semigroup $\mathcal{G}$ on which a ("congruence-type") equivalence relation $\sim$ is given such that $ab \sim a'b'$ whenever $a \sim a'$, $b \sim b'$, and such that the corresponding set $\Gamma = \mathcal{G}/_{\sim}$ of equivalence classes $[a]$ $(a \in \mathcal{G})$ forms a *finite abelian group* under the operation

$$[a][b] = [ab].$$

In such a case, $(\mathcal{G}, \sim)$ or $(\mathcal{G}, \Gamma)$ is called an **(arithmetical) formation**, with **class group** $\Gamma$, and **class number** $h = \text{card}\,\Gamma$.

A few examples of formations are provided by:

(i) $(\mathcal{G}, =)$ for which $\Gamma$ is trivial, $h = 1$;

(ii) $(\mathbb{N}\langle m\rangle, \equiv \pmod{m})$, where $\mathbb{N}\langle m\rangle$ is the set of all natural numbers coprime to a given $m \in \mathbb{N}$, and $h = \phi(m)$;

(iii) $(\mathcal{G}_K, \sim)$, where $\mathcal{G}_K$ is the semigroup of all integral ideals of a given algebraic number field $K$, $\sim$ denotes standard ideal class equivalence in $\mathcal{G}_K$, and $h$ is the standard class number $h_K$ of $K$.

The type of analytic number theory developed for formations $(\mathcal{G}, \sim)$ in [AB], Chapter 9, is concerned with those formations that satisfy **Axiom** $\mathcal{A}^*$. *There exist constants $A > 0$, $\delta > 0$, and $\eta$ with $0 \le \eta < \delta$, such that for any class $\alpha \in \Gamma$*

$$\#\{a \in \alpha : |a| \le x\} = \frac{A}{h} x^{\delta} + O(x^{\eta}) \quad \textit{as} \quad x \to \infty.$$

This axiom is then equivalent to the two conditions:

(i) *$\mathcal{G}$ satisfies Axiom $\mathcal{A}$ of* [AB]:

$$\#\{a \in \mathcal{G} : |a| \le x\} = Ax^{\delta} + O(x^{\eta}) \textit{ as } x \to \infty$$

*for constants $A > 0$, $\delta > 0$ and $\eta$ with $0 \le \eta < \delta$*, and

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

(ii) *for any classes* $\alpha$, $\alpha'$ *in* $\Gamma = \mathcal{G}/_{\sim}$,

$$\lim_{x\to\infty} \#\{a \in \alpha : |a| \leq x\}/\#\{a' \in \alpha' : |a'| \leq x\} = 1.$$

Although previous authors such as those cited above implicitly or explicitly investigated asymptotic consequences of Axiom $\mathcal{A}^*$ in general, certain particular aspects of the development in [AB], Chapter 9, are restricted to formations which satisfy a certain *additional* Axiom $\mathcal{A}^{**}$, which encompasses *all* the natural motivating examples described in that chapter – this simplifies the approach to the applications of immediate interest, but could also be viewed as an introduction to the more theoretical general case.

The analytic theory of *additive* arithmetical formations initiated by Halter–Koch and Warlimont [1] provides both an analogue of the previous theory, and an extension of earlier research on rational or algebraic function fields over a finite field, going back to work of Kornblum [1] and E. Artin [1] more than 75 years ago, followed by Hayes [1] in 1965.

Following Halter–Koch and Warlimont [1] (without *continual* further citations to that paper), first define an **additive (arithmetical) formation** to be a triple $(\mathcal{G}, \sim, f_0)$ such that $(\mathcal{G}, \sim)$ is a formation for which $\mathcal{G}$ is an additive arithmetical semigroup, and for some $n_0 \in \mathbb{N}$ there is given a group epimorphism

$$f_0 : \Gamma \to \mathbb{Z}/n_0\mathbb{Z}$$

with the property that $\partial(a) \in f_0(\alpha)$ for all $\alpha \in \Gamma$ and $a \in \alpha$. (If $(\mathcal{G}, \sim)$ is a formation with $\mathcal{G}$ additive, and $n_0 = \gcd\{\partial(a) : a \sim 1\}$, then it is fairly easily shown that there exists a unique group homomorphism $f_0 : \Gamma \to \mathbb{Z}/n_0\mathbb{Z}$ with $f_0([a]) = \partial(a) + n_0\mathbb{Z}$, and $f_0$ is surjective if $1 = \gcd\{\partial(a) : a \in \mathcal{G}\}$.)

An additive counterpart to Axiom $\mathcal{A}^*$ then provided by **Axiom** $(\mathcal{A}^{\#})^*$. *There exist constants* $B > 0$, $q > 1$, *and* $\nu$ *with* $0 \leq \nu < 1$, *such that for* *any class* $\alpha \in \Gamma$ *and* $k \in f_0(\alpha)$

$$\alpha(k) := \#\{a \in \alpha : \partial(a) = k\} = \frac{B}{h} q^k + O(q^{\nu k}) \quad \textit{as} \quad k \to \infty.$$

If this axiom (referred to below as *Axiom* $\mathcal{B}$, for short) is satisfied, it can be deduced that the assumed constant $n_0 \in \mathbb{N}$ *must* equal the gcd $\{\partial(a) : a \sim 1\}$, *and*, for any $k \in \mathbb{N}$,

$$G(k) = \frac{B}{n_0} q^k + O(q^{\nu k}) = \frac{Ah}{n_0} q^k + O(s^k) \quad \text{as} \quad k \to \infty,$$

in terms of the preferred notation $A = B/h$ and $s = q^\nu$ of Halter-Koch and Warlimont.

Just as the investigation of asymptotic consequences of Axiom $\mathcal{A}^*$ is aided by the study of analytical properties of so-called *L-series*, the investigation of consequences of Axiom $\mathcal{B}$ is aided by studies of the **relative** *zeta functions*

$$Z(y, \chi) = \sum_{k=0}^{\infty} \left( \sum_{\partial(a)=k} \chi(a) \right) y^k,$$

relative to the *characters* $\chi$ of $\Gamma$ (i.e. the group homomorphisms $\chi$ of $\Gamma$ into the multiplicative group of non-zero complex numbers).

Analytical studies of these new zeta functions $Z(y, \chi)$ turn out to be rather technical and subtle. For the purposes of establishing an appropriate abstract prime number theorm for additive formations (or *prime element theorem*, for short), additive arithmetical formations are classified into **types** I or II according as no zeta function $Z(y, \chi)$ has zeros on the circle $|y| = q^{-1}$, or else some zeta function does have such zeros. (Under Axiom $\mathcal{B}$, each $Z(y, \chi)$ is meromorphic for $|y| < s^{-1}$, and has no zeros for $|y| < q^{-1}$.)

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

By means of delicate arguments, Halter–Koch and Warlimont derive a prime element theorem for both types, of which the "more classical" type I case has the following form:

(8.7.1) PRIME ELEMENT THEOREM FOR TYPE I FORMATIONS. *Let* $(\mathcal{G}, \sim, f_0)$ *be an additive formation satisfying Axiom* $\mathcal{B}$. *Let* $r$ *with* $s < r < q$ *be such that no zeta function* $Z(y, \chi)$ *has a zero on* $|y| = r^{-1}$, *but* $Z(y, \chi)$ *has a zero* $y$ *with* $q^{-1} < |y| < r^{-1}$ *if it has one with* $q^{-1} < |y| < s^{-1}$. *Also suppose that the formation is of type I, and let* $\xi \geq \max(r, \sqrt{q})$. *Then the prime element function*

$$\begin{aligned} P_\alpha(k) : &= \#\{p \in \mathcal{P} \cap \alpha : \partial(p) = k\} \\ &= \frac{n_0}{h} \frac{q^k}{k} + O\left(\frac{\xi^k}{k}\right) \quad \textit{for all} \quad \alpha \in \Gamma \quad \textit{and} \quad k \in f_0(\alpha) \end{aligned} \tag{7.1}$$

*if and only if no zeta function* $Z(y, \chi)$ *has a zero with* $|y| < \xi^{-1}$.

For type II formations, an analysis more delicate than one given by Halter–Koch and Warlimont can show

(8.7.2) THEOREM.

*(i) If the zeta function* $Z(y, \chi_0)$ *with the principal character* $\chi_0$ *has a zero at* $-q^{-1}$ *then*

$$P_\alpha(k) = \frac{n_0}{h} \frac{q^k}{k} \left(1 - (-1)^k\right) + O\left(\frac{\xi_0^k}{k}\right) \tag{7.2}$$

*for all* $\alpha \in \Gamma$ *and* $k \in f_0(\alpha)$, *where* $\xi_0 = \max\{r, \sqrt{q}\}$ *and*

*(ii) If* $Z(y, \chi_0)$ *does not have zeros at* $-q^{-1}$ *then*

$$P_\alpha(k) = \frac{n_0}{h} \frac{q^k}{k}(1 - z_0^k) + 0\left(\frac{\xi_0^k}{k}\right), \tag{7.3}$$

*where* $q^{-1}z_0$ *is the only zero of some zeta function* $Z(y, \chi)$ *on the circle* $|y| = q^{-1}$ *and the character* $\chi$ *is identically 1 on the* $\ker(f_0)$.

This result is a refinement of the result of Halter–Koch and Warlimont and a generalization of a theorem of Indlekofer–Manstavicious–Warlimont [1], i.e., Theorem 5.1.1 of this book.

Zhang [9] has investigated further conditions which lead to type I formations and conclusions like (7.1).

(8.7.3) THEOREM. *An additive formation* $(\mathcal{G}, \sim, f_0)$ *is of type I, if any of the following two conditions is satisfied:*

*(i) There exists constant* $B > 0$ *and* $q > 1$ *such that*

$$\sum_{\alpha\in\Gamma} \sum_{\substack{k\geq 1 \\ k\in f_0(\alpha)}} \left(\alpha(k) - \frac{B}{h}q^k\right)^2 q^{-k} < \infty;$$

*(ii) There exists constants* $B > 0$ *and* $q > 1$ *such that*

$$\alpha(k) = \frac{B}{h}q^k + O_v(q^{vk})$$

*for every* $\alpha \in \Gamma$ *and* $k \in f_0(\alpha)$ *with every fixed* $v > \frac{1}{2}$. *Also, for every character* $\chi$,

$$\liminf_{x\to q^{-\frac{1}{2}}-} \left(1 - q^{\frac{1}{2}}x\right) Z\left(\pm\chi(\alpha_1^{-1})x, \chi\right) Z\left(\chi^2(\alpha_1^{-1})x, \chi^2\right) \leq 0,$$

*where* $\alpha_1$ *is an arbitrarily fixed congruence class satisfying* $\partial(\alpha_1) \subset 1 + n_0\mathbb{Z}$.

This theorem is a generalization of Theorems 3.5.1 and 3.5.6 together. Both Halter–Koch and Warlimont, and Zhang, also discuss applications to important special formations arising from *algebraic function fields* over a finite field.

Lastly, Halter–Koch and Warlimont [1] establish (i) an *"Inversion Theorem"* to the effect that the conclusions of their prime element theorems for both types of formations are essentially equivalent to Axiom $\mathcal{B}$, and (ii) a *"Realization Theorem"* showing how to formally construct additive formations satisfying Axiom $\mathcal{B}$ with $\sqrt{q} < s < q$, given any group epimorphism $f_0 : \Gamma \to \mathbb{Z}/n_0\mathbb{Z}$ of an arbitrary finite abelian group $\Gamma$ onto some quotient group $\mathbb{Z}/n_0\mathbb{Z}$ of $(\mathbb{Z}, +)$.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

# BIBLIOGRAPHY

APOSTOL, T.M.

[1] *Introduction to Analytic Number Theory.* Springer–Verlag, New York, Heidelberg, Berlin, 1976.

ARTIN, E.

[1] Quadratische Körper im Gebiete der höreren Kongruenzen, I–II. *Math. Z.*, **19** (1924), 153–246.

BATEMAN, P.T. AND H.G. DIAMOND

[1] Asymptotic distribution of Beurling's generalized prime numbers. In: *Studies in Number Theory*, Vol. **6**, Math. Assoc. Amer., Prentice-Hall, Englewood Cliffs, N.J., 1969, 152–210.

BEURLING, A.

[1] Analyse de la loi asymptotique de la distribution des nombres premiers généralisés, I. *Acta Math.*, **68** (1937), 255–291.

BILLINGSLEY, P.

[1] *Probability and Measure.* 2nd edition, John Wiley and Sons, New York, 1986.

[2] The probability theory of additive arithmetic functions. *Ann. of Prob.*, **2** (1974), 749–791.

BOMBIERI, E.

[1] Sull'analogo della formula di Selberg nei corpi di funzioni. *Atti Accad. Naz. Lincei Rend. cl. Sci. Fis. Mat. Natur.*, (8) **35** (1963), 252–257.

[2] Correction to my paper "Sull'analogo della formula di Selberg nei corpi di funzioni". *Atti Accad. Naz. Lincei Rend. Cl. Sci. Fis. Mat. Natur.*, (9) **1** (1990), 177–179.

[3] Hilbert's 8th problem: an analogue. Proceedings of Symposia in Pure Mathematics of AMS, Vol. 28, 1976, 269–274.

CAR, M.

[1] Théorèmes de densité dans $F_q[X]$. *Acta Arith.*, **48** (1987), 145–165.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

CARLITZ, L.

[1] The arithmetic of polynomials in a Galois field. *Amer. J. Math.*, **54** (1932), 39–50.

[2] On Polynomials in a Galois Field. *Bull. Amer. Math. Soc.*, **38** (1932), 736–744.

[3] Some topics in the arithmetic of polynomials. *Bull. Amer. Math. Soc.*, **48** (1942), 679-691.

[4] The distribution of irreducible polynomials in several indeterminates. *Illinois J. Math.*, **7** (1963), 371–375.

[5] Rings of arithmetic functions. *Pacific J. Math.*, **14** (1964), 1165–1171.

[6] The distribution of irreducible polynomials in several indeterminates, II. *Can. J. Math.*, **17** (1965), 261–266.

[7] Arithmetic functions in an unusual setting, I–II. *Am. Math. Monthly*, **73** (1966), 582–590, and *Duke Math. J.*, **34** (1967), 757–760.

CARLITZ, L. AND E. COHEN

[1] Divisor functions of polynomials in a Galois field. *Duke Math. J.*, **14** (1947), 13–20.

[2] Cauchy products of divisor functions in $GF[p^n, x]$. *Duke Math. J.*, **14** (1947), 707–722.

CHANDRASEKHARAN, K.

[1] *Arithmetical Functions*, Springer–Verlag, 1970.

COHEN, E.

[1] A class of arithmetical functions. *Proc. Nat. Acad. Sci. U.S.A.*, **41** (1955), 939–944.

[2] On the inversion of even functions of finite abelian groups (mod $H$). *J. Reine Angew. Math.*, **207** (1961), 192–202.

[3] Almost even functions of finite abelian groups. *Acta Arith.*, **7** (1962), 311–323.

[4] Fourier expansions of arithmetical functions. *Bull. Am. Math. Soc.*, **67** (1961), 145–147.

COHEN, S.D.

[1] Some arithmetical functions in finite fields. *Glasgow Math. J.*, **11** (1969), 21–36.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

[2] Further arithmetical functions in finite fields. *Proc. Edinburgh Math. Soc.*, **16** (2) (1969), 349–363.

[3] Uniform distribution of polynomials over finite fields. *J. London Math. Soc.*, (2) **6** (1972), 93–102.

[4] The function field abstract prime number theorem, *Math. Proc. Cambr. Phil. Soc.*, **106** (1989), 7–12.

COURANT, R. AND D. HILBERT

[1] *Methods of Mathematical Physics.* Vol. I, Interscience Publishers, New York, 1953.

DELANGE, H.

[1] Sur les fonctions arithmétiques multiplicatives. *Ann. Sci. de l'École Norm. Sup.*, **78** (1961), 273–304.

[2] On a class of multiplicative arithmetical functions. *Scripta Math.*, **26** (1963), 121–141.

DEURING, M.

[1] *Lectures on the Theory of Algebraic Functions of One Variable.* Spinger-Verlag, Berlin, 1973.

DIAMOND, H.G.

[1] The prime number theorem for Beurling's generalized numbers. *J. Number Theory*, **1** (1969), 200–207.

[2] Asymptotic distribution of Beurling's generalized integers. *Illionois J. Math.*, **14** (1970), 12–28.

[3] A set of generalized numbers showing Beurling's theorem to be sharp. *Illinois J. Math.*, **14** (1970), 29–34.

[4] When do Beurling generalized integers have a density? *J. Reine Angew Math.*, **295** (1977), 22–39.

DIXON, J.D.

[1] The number of steps in the Euclidean algorithm. *J. Number Th.*, **2** (1970), 414–422.

EICHLER, M.

[1] *Introduction to the Theory of Algebraic Numbers and Functions.* Academic Press, New York, 1966.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

ELLIOTT, P.D.T.A.

[1] *Probabilistic Number Theory*, Vols. I–II. Springer, Berlin, 1979/80.

ERDŐS, P.

[1] On a tauberian theorem connected with the new proof of the prime number theorem. *J. Indian Math. Soc.*, **13** (1949), 131–147.

ERDŐS, P. AND M. KAC

[1] On the Gaussian law of errors in the theory of additive functions. *Proc. Nat. Acad. Sci. U.S.A.*, **25** (1939), 206–207.

[2] The Gaussian law of errors in the theory of additive number-theoretic functions. *Amer. J. Math.*, **62** (1940), 738–742.

ERDŐS, P., SAFFARI, B. AND R.C. VAUGHAN

[1] On the asymptotic density of sets of integers, II. *J. London Math. Soc.*, (2) **19** (1979), 17–20.

ERDŐS, P. AND A. WINTNER

[1] Additive arithmetical functions and statistical independence. *Amer. J. Math.*, **61** (1939), 713–721.

FOGELS, E.

[1] On the distribution of analogues of primes. (In Russian) *Dokl. Akad. Nauk SSSR*, **146** (1962), 318–321.

[2] On the distribution of prime ideals. *Acta Arith.*, **7** (1962), 255–269.

[3] On the zeros of $L$–functions. *Acta Arith.*, **11** (1965), 67–96.

[4] On the abstract theory of primes, I–III. *Acta Arith.*, **10** (1964), 137–182, 333–358 and **11** (1966), 292–331.

FORMAN, W. AND H.N. SHAPIRO

[1] Abstract prime number theorems. *Commun. Pure Appl. Math.*, **7** (1954), 587–619.

FRIESEN, C. AND D. HENSLEY

[1] The statistics of continued fractions for polynomials over a finite field. *Proc. Amer. Math. Soc.*, **124** (1996), 2661–2673.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

GNEDENKO, B.V. AND A.N. KOLMOGOROV

[1] *Limit Distributions for Sums of Independent Random Variables.* Translated from the Russian and annoted by K.L. Chung, Addison-Wesley, Reading, Mass., London, 1968.

GOSS, D.

[1] *Basic Structures of Function Field Arithmetic.* Springer, 1996.

GRANVILLE, A.

[1] Solution of a problem of Bombieri. *Atti Accad. Naz. Lincei. Rend. cl. Sci. Fis. Mat. Natur.*, (2) **4** (1993), 181–183.

GREENE, D.H. AND D.E. KNUTH

[1] *Mathematics for the Analysis of Algorithms.* 3rd Ed., Birkhäuser, 1990.

HALÁSZ, G.

[1] Über die Mittelwerte multiplikativer zahlentheoretischer Funktionen. *Acta Math. Acad. Sci. Hung.*, **19** (1968), 365–403.

[2] On the distribution of additive and the mean values of multiplicative arithmetic functions. *Studia Scient. Math. Hungarica*, **6** (1971), 211–233.

[3] On the distribution of additive arithmetic functions. *Acta Arithmetica*, **27** (1975), 143–152.

HALBERSTAM, H. AND H.-E. RICHERT

[1] *Sieve Methods.* Academic Press, 1974.

[2] A Weighted Sieve of Greaves' Type I, in: *Elementary and Analytic Theory of Numbers*, Banach Center Publications, Vol. 17, 1985, Warsaw, 155–182.

HALL, R.R.

[1] *Sets of Multiples.* Cambridge Univ. Press, 1996.

HALL, R.S.

[1] The prime number theorem for generalized primes. *J. Number Theory*, **4** (1972), 313–320.

[2] Beurling generalized prime number systems in which the Chebyshev inequalities fail. *Proc. Am. Math. Soc.*, **40** (1973), 79–82.

HALTER-KOCH, F. AND R. WARLIMONT

[1] Analytic number theory in formations based on additive arithmetical semigroups. *Math. Zeitschr.*, **215** (1994), 99–128.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Hardy, G.N.

[1] A note on Ramanujan's trigonometrical function $c_q(n)$ and certain series of arithmetical functions. *Proc. Cambridge Philos. Soc.*, **20** (1921), 263–271.

Hayes, D.R.

[1] The distribution of irreducibles in $GF_{[q,x]}$. *Trans. Am. Math. Soc.*, **117** (1965), 101–127.

Heilbronn, H.

[1] On the average length of a class of finite continued fractions. In: *Number Theory and Analysis*, Plenum Press, 1969, pp.87–96.

Hildebrand, A. and G. Tenenbaum

[1] On some Tauberian theorems related to the prime number theorem. *Compositio Math.*, **90** (1994), 315–349.

Indlekofer, K.-H.

[1] The abstract prime number theorem for function fields. *Acta Math. Hung.*, **62** (1993), 137–148.

Indlekofer, K.-H., Knopfmacher, J. and R. Warlimont

[1] Arithmetical semigroups, I: direct factors. *Manuscr. Math.*, **71** (1991), 83–96.

Indlekofer, K.-H. and E. Manstavicius

[1] Additive and multiplicative functions on arithmetical semigroups. *Publ. Math. Debrecen*, **45** (1994), 1–17.

[2] New approach to multiplicative functions on arithmetical semigroups. *Lithuanian Math. J.*, **34** (1994), 356–363.

Indlekofer, K.-H., E. Manstavicius and R. Warlimont

[1] On a certain class of infinite products with an application to arithmetical semigroups. *Arch. Math.*, **56** (1991), 446–453.

Iwaniec, H.

[1] Rosser's sieve. *Acta Arith.*, **36** (1980), 171–202.

Jacobson, N.

[1] *Theory of Rings*. Am. Math. Soc., Providence, R.I., 1943.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

KNOPFMACHER, A.

[1] The length of the continued fraction expansion for a class of rational functions in $\mathbb{F}_q(X)$. *Proc. Edin. Math. Soc.*, **34** (1991), 7–17.

KNOPFMACHER, A. AND J. KNOPFMACHER

[1] The exact length of the Euclidean algorithm in $\mathbb{F}_q[X]$. *Mathematika*, **35** (1988), 297–304.

[2] Counting polynomials with a given number of zeros in a finite field. *Linear and Mult. Algebra*, **26** (1990), 287–292.

[3] Counting irreducible factors of polynomials over a finite field. *Discr. Math.*, **112** (1993), 103–118.

KNOPFMACHER, A., KNOPFMACHER, J. AND R. WARLIMONT

[1] "Factorisatio numerorum" in arithmetical semigroups. *Acta Arith.*, **61** (1992), 327–336.

[2] Ordered factorizations for integers and arithmetical semigroups. In: *Advances in Number Theory.* Proc. 3rd Conf. of Canadian Number Th. Assoc., 1991, *Eds.* F. Gouvêa and N. Yui, Clarendon Press, Oxford, 1993, pp.151–161.

[3] Lengths of factorizations for polynomials over a finite field. *Contemp. Math.*, **168** (1994), 185–206.

KNOPFMACHER, A. AND J.N. RIDLEY

[1] Reciprocal sums over partitions and compositions. *SIAM J. Discrete Math.*, **6** (1993), 388–399.

KNOPFMACHER, A. AND R. WARLIMONT

[1] Distinct degree factorizations for polynomials over a finite field. *Trans. Amer. Math. Soc.*, **347** (1995), 2235–2243.

[2] Distinct degree factorizations in arithmetical semigroups. *Manuscripta Math.*, **87** (1995), 481–487.

[3] Counting permutations and polynomials with a restricted factorization pattern. *Australasian J. of Combinatorics* **13** (1996), 151–162.

KNOPFMACHER, J.

[AB] *Abstract Analytic Number Theory.* North-Holland Publ. Co., Amsterdam, 1975; Second Edition, Dover Publ., New York, 1996.

[1] Arithmetical properties of finite rings and algebras, and analytic number theory, III. *J. Reine Angew. Math.* **259** (1973), 157–170.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

[2] Direct factors of polynomial rings over finite fields. *J. Combin. Th.*, **A40** (1985), 429–434.

[3] Arithmetical properties of finite rings and algebras, and analytic number theory, IV: Relative asymptotic enumeration and $L$–series. *J. Reine Angew. Math.*, **270** (1974), 97–114.

[4] Arithmetical properties of finite rings and algebras, and analytic number theory, V: Categories and relative analytic number theory. *J. Reine Angew. Math.*, **271** (1974), 95–121.

[5] Finite modules and algebras over rings of algebraic functions. *Bull. London Math. Soc.*, **8** (1976), 289–293.

[6] An abstract prime number theorem relating to algebraic function fields. *Arch. der Math.*, **29** (1977), 271–279.

[7] Fourier analysis of arithmetical functions. *Ann. Mat. Pura Appl.*, **109** (1976), 177–201.

[8] *Analytic arithmetic of algebraic function fields*, Lecture Notes in Pure and Applied Mathematics, Vol. 50, Marcel Dekker, New York, Basel, 1979.

Knopfmacher, J. and P.G. Slattery

[1] Ramanujan expansions over additive arithmetical semigroups. *Bull. Soc. Math. Belg.*, **B41** (1989), 109–127.

Knopp, K.

[1] *Theory and Application of Infinite Series.* Dover, 1990; *Theory and Applications of Infinite Series.* Blakie and Son Ltd., London, 1951.

Knuth, D.E.

[1] *The Art of Computer Programming*, Vol. **2**, 2nd edition, Addison-Wesley, 1981.

Kornblum, H.

[1] Über die Primfunktionen in einer arithmetische Progession. *Math. Zeitschr.*, **5** (1919), 100–111.

Kubilius, J.

[1] *Probabilistic Methods in the Theory of Numbers.* Am. Math. Soc. Transl. of Math. Monographs, No. 11, Providence, (1964).

Lidl, R. and H. Niderreiter

[1] *Finite Fields.* Cambridge Univ. Press, Cambridge, 1984.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

LUCHT, L.

[1] Ramanujan expansions revisited. *Arch. Math.*, **64** (1995), 121–128.

[2] Weighted relationship theorems and Ramanujan expansions. *Acta Arith.*, **70** (1995), 25–42.

MAUCLAIRE, J.-L.

[1] Integration and number theory. *Prospects of Math. Sci., World Sci. Publ.*, (1988), 97–125.

MANSTAVICIUS, E.

[1] Semigroup elements free of large prime factors. In: *New Trends in Probability and Statistics* (ed. by F. Schweiger and E. Manstavicius), TEV, Vilnius/VSP, Utrecht, 1992, pp.135–153.

[2] Remarks on the semigroup elements free of large prime factors. *Lithuanian Math. J.*, **32** (1992), 400–409.

MÜLLER, H.

[1] Über abstrakte Primzahlsätze mit Restglied. Thesis, Freie Universität, Berlin (1970).

[2] Ein Beitrag zur abstrakten Primzahltheorie. *J. Reine Angew. Math.*, **259** (1973), 171–182.

[3] Über die asymptotische Verteilung von Beurlingshe Zahlen. *J. Reine Angew. Math.*, **289** (1977), 181–187

OPPENHEIM, A.

[1] On an arithmetic function. *J. London Math. Soc.*, **1** (1926), 205–211, and **2** (1927), 123–130.

PARZEN, E.

[1] *Modern Probability Theory and its Applications.* John Wiley & Sons, New York, 1960.

PÓLYA, G. AND G. SZEGŐ

[1] *Problems and Theorems in Analysis.* Grundlehren der mathematischen Wisenschaften **193**, Springer-Verlag, Berlin, New York, 1976–78.

RAMANUJAN, S.

[1] On certain trigonometrical sums and their applications in the theory of numbers. *Trans. Cambridge Philos. Soc.*, **22** (1918), 259–276.

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

RIDLEY, J.N. AND D.B. SEARS

[1] Asymptotic and exact analytic formulae for enumerating modules. *Arch. der Math.*, **32** (1979), 149–154.

RYAVEC, C.

[1] Euler products associated with Beurling's generalized prime number systems. *Proc. Symp. Pure Math.,* **24** (1973), 263–266.

SAFFARI, B.

[1] On the asymptotic density of sets of integers. *J. London Math. Soc.*, (2) **13** (1976), 475–485.

SCHWARZ, W.

[1] Fourier–Ramanujan–Entwicklungen zahlentheoretischer Funktionen und Anwendungen. In: *Festschrift Wiss. Ges. Univ. Frankfurt a.M.*, (1981), 399–415.

[2] Ramanujan expansions of arithmetical functions. In: *Ramanujan Revisited* (G.E. Andrews, et al., *eds.*). Academic Press (1988), 187–214.

SCHWARZ, W. AND J. SPILKER

[1] *Arithmetical Functions.* Cambridge Univ. Press, 1994.

SHADER, L.

[1] Arithmetic functions associated with unitary divisors in $GF_{[q,x]}$, I–II. *Ann. Mat. Pura Appl.*, **86** (1970), 79–98.

SLATTERY, P.G.

[1] *Ramanujan Expansions over Arithmetical Semigroups*, Ph.D. Thesis, University of the Witwatersrand, Johannesburg, S. Africa, 1989.

THOMAS, A.D.

[1] *Zeta Functions – An Introduction to Algebraic Geometry.* Pitman Publ. Co., London, 1977.

TITCHMARSH, E.C.

[1] *The Theory of Functions.* Oxford Univ. Press, London, 1952.

VAN AARDENNE–EHRENFEST, T., DE BRUIJN, N.G. AND J. KOREVAAR

[1] A note on slowly oscillating functions. *Niew Arch. Wiskunde*, (2) **23** (1949), 77–86.

van Lint, J.H. and R.M. Wilson

[1] *A Course in Combinatorics.* Cambridge Univ. Press, New York, 1992.

Warlimont, R.

[1] Arithmetical semigroups, II: Sieving by large and small prime elements. Sets of multiples. *Manuscr. Math.*, **71** (1991), 197–221.

[2] Arithmetical semigroups, IV: Selberg's analysis. *Arch. Math.*, **60** (1993), 58–72.

[3] Arithmetical semigroups, III: Elements with prime factors in residue classes. *Monatsh. Math.*, **119** (1995), 239–247.

[4] Arithmetical semigroups V: multiplicative functions. *Manuscr. Math.*, **77** (1992), 361–383.

[5] Tauberian theorems for two real sequences linked by a convolution. *Math. Nachr.*, **193** (1998), 211–234.

[6] Tauberian theorems for two real sequences linked by a convolution, II. *Arch. Math.*, **73** (1999), 265–272.

Weil, A.

[1] Sur les courbes algebriques et les varietés qui s'en deduisent. *Actualités sci. et ind.*, **1041** (1948).

Wintner, A.

[1] *The Theory of Measure in Arithmetical Semigroups.* Waverly, Baltimore, Md., 1944.

Wirsing, E.

[1] Elementare Beweise des Primzahlsatzes mit Restglid, II. *J. Reine Angew. Math.*, **214/215** (1964), 1–18.

[2] Das asymptotische Verhalten von Summen über multiplikative Funktionen, II. *Acta Math. Acad. Sci. Hung.*, **18** (1967), 411–467.

Zhang, W.-B.

[1] The abstract prime number theorem for algebraic function fields, In: Analytic Number Theory (B.C. Berndt et al. eds.), Prog. Math. 85, Birkhäuser, 1990, 529–558.

[2] A Chebyshev type upper estimate for prime elements in additive arithmetic semigroups. *Monatsh. Math.*, **129** (2000), 227–260.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

[3] Probabilistic number theory in additive arithmetic semigroups. In: *Analytic Number Theory* (B.C. Berndt et al. eds.) Prog. Math., Birkhäuser, 1996, 839–884.

[4] Elementary proofs of the abstract prime number theorem for algebraic function fields. *Trans. Amer. Math. Soc.*, **332** (1992), 923–937.

[5] Probabilistic number theory in additive arithmetic semigroups, II., to appear in *Math. Zeitschr.*

[6] The prime element theorem in additive arithmetic semigroups, I. *Illinois J. Math.*, **40** (1996), 245–280.

[7] The prime element theorem in additive arithmetic semigroups, II. *Illinois J. Math.*, **42** (1998), 198–229.

[8] Mean–value theorems of multicative functions on additive arithmetic semigroups, *Math. Zeitschr.*, **229** (1998), 195–233.

[9] The prime element theorem on additive formations. *Math. Zeitschr.*, **231** (1999), 457–478.

[10] A generalization of Halász's theorem to Beurling's generalized integers and its application. *Illinois J. Math.*, **31** (1987), 645–664.

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

# NOTATIONS

| *Notation* | *Section* | *Interpretation* |
|---|---|---|
| $\mathbb{N}$ | – | the (set of) positive integers |
| $\mathbb{Z}$ | – | the integers |
| $\mathbb{Q}$ | – | the rational numbers |
| $\mathbb{R}$ | – | the real numbers |
| $\mathbb{C}$ | – | the complex numbers |
| $\mathbb{Z}/n\mathbb{Z}$ | – | the quotient ring of $\mathbb{Z}$ modulo ideal $n\mathbb{Z}$ |
| $O(\quad)$ | – | big oh notation |
| $o(\quad)$ | – | little oh notation |
| $\ll$ | – | Vinogradov's notation for $O(\quad)$ |
| $\mathcal{G}$ | – | additive arithmetical semigroup |
| $\mathcal{P}$ | – | the primes in $\mathcal{G}$ |
| $\partial$ | – | the integer-valued degree mapping on $\mathcal{G}$ |
| $G^{\#}(n), G(n)$ | – | number of elements of degree $n$ in $\mathcal{G}$ |
| $P^{\#}(n), P(n)$ | – | number of primes of degree $n$ in $\mathcal{G}$ |
| $Z_{\mathcal{G}}(y), Z(y)$ | – | the enumerating, or generating, or zeta function of $\mathcal{G}$ |
| $Z(y, \chi)$ | 8.7 | the zeta function associated with character $\chi$ of additive arithmetical formation $\mathcal{G}$ |
| $\mathbb{F}_q$ | 1.1, 2.1, 8.1, 8.5 | the finite field with $q$ elements |
| $\mathbb{F}_q[X]$ | 1.1, 2.1, 2.2 | the ring of polynomials in $X$ over $\mathbb{F}_q$ |
| $\mathbb{F}_q[X_1, \ldots, X_k]$ | 1.1 | the ring of polynomials in $X_1, \ldots, X_k$ over $\mathbb{F}_q$ |
| $\mathcal{G}_q$ | 1.1, 2.2, 8.1, 8.4, 8.5 | the additive arithmetical semigroup of monic polynomials in $\mathbb{F}_q[X]$ |

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

| *Notation* | *Section* | *Interpretation* |
|---|---|---|
| $G_q^{\#}(n)$ | 1.1 | number of elements of degree $n$ in $\mathcal{G}_q$ |
| $\mathcal{F}_q$ | 1.1, 2.1 | the category of finitely-generated torsion modules over $\mathbb{F}_q[X]$ |
| $\mathcal{F}_q(n)$ | 1.1 | number of non-isomorphic modules of cardinal $q^n$ in $\mathcal{F}_q$ |
| $\mathcal{S}_q$ | 1.1, 2.1 | the class of semi-simple $D$-algebras of finite cardinal when $D = \mathbb{F}_q[X]$ |
| $\mathcal{S}_q(n)$ | 1.1, 2.1 | number of non-isomorphic algebras of cardinal $q^n$ in $\mathcal{S}_q$ |
| $K$ | 1.1 | the field of algebraic functions in one variable over $\mathbb{F}_q$ |
| $\mathcal{G}_K$ | 1.1 | the additive arithmetical semigroup of integral divisors in $K$ |
| $\zeta_K$, $\zeta_K(z)$ | 1.1 | the zeta function of $K$ |
| $D$ | 1.1 | the ring of integral functions in $K$ |
| $\mathcal{G}_D$ | 1.1 | the additive arithmetical semigroup of non-zero ideals of $D$ |
| $\zeta_D(z)$ | 1.1 | the zeta function of $\mathcal{G}_D$ |
| $\mathcal{F}_D$ | 1.1, 2.1 | the category of finitely-generated torsion modules over $D$ |
| $\mathcal{S}_D$ | 1.1 | the class of semi-simple finite algebras over $D$ |
| $\mathcal{H}_{q,2}$ | 1.1 | the additive arithmetical semigroup of associate classes of homogeneous polynomials in $\mathbb{F}_q[X_1, X_2]$ |
| $Z_q(y), Z_D(y), Z_{\mathcal{F}}(y)$ | 2.1 | generating functions of $\mathcal{G}_q$, $\mathcal{G}_D$, $\mathcal{F}$, resp. |
| $\gamma$ | 1.2, 3.1 | classical Euler constant |
| $\gamma_G$ | 1.2 | Euler constant of $\mathcal{G}$ |
| $\gamma_{\mathcal{G}_K}$ | 1.2 | Euler constant of $\mathcal{G}_K$ |
| $\gamma_{\mathcal{G}_D}$ | 1.2 | Euler constant of $\mathcal{G}_D$ |
| $\gamma_i$, $\gamma_i(\mathcal{G})$ | 1.2 | generalized Euler constants of $\mathcal{G}$ |
| $\mathcal{G}_{(k)}$ | 1.3, 4.1, 8.2 | the subset of $k$-free elements of $\mathcal{G}$ |
| $\mathcal{G}_{\langle k \rangle}$ | 1.1 | the subset of $\mathcal{G}$ of elements coprime to $k$ in $\mathcal{G}$ |

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

| *Notation* | *Section* | *Interpretation* |
|---|---|---|
| $\bar{f}(n)$, $F(n)$ | 1.3 | summatory function of $f(a)$ with $\partial(a) = n$ |
| $m_f$, $m(f)$ | 1.3, 6.4 | (asymptotic) mean-value of $f$ |
| $\delta$, $\delta(E)$ | 1.3, 4.1, 8.2 | asymptotic density of subset $E$ |
| $f^{\#}(y)$, $\hat{F}(y)$ | 1.3, 6.1, 6.2, 6.3, 6.4, 6.6 | generating function of $f$ on $\mathcal{G}$ |
| $d_k(a)$ | 1.3 | number of factorizations $b_1 b_2 \cdots b_k = a$ |
| $d_*(a)$ | 1.3 | number of divisors $d$ of $a$ for which $d$ and $a/d$ are coprime |
| $\bar{d}(N)$, $\overline{d_*}(N)$, $\overline{d_k}(N)$ | 2.2 | summatory functions of $d(a)$, $d_*(a)$, $d_k(a)$, resp. |
| $d^{\#}(y)$, $d_*^{\#}(y)$, $d_k^{\#}(y)$ | 2.2 | generating functions of $d(a)$, $d_*(a)$, $d_k(a)$, resp. |
| $\phi_*(a)$ | 1.5 | number of elements of the same degree as $a$ and coprime to $a$ in $\mathcal{G}$ |
| $\sigma_*(a)$ | 1.5 | sum of degrees of divisors of $a$ |
| $f * g$ | 3.1, 6.1 | convolution of arithmetical functions $f$ and $g$ |
| $L$, $Lf$ | 3.1, 6.1 | differentiation operator on arithmetical functions |
| $\Lambda(a)$ | 3.1 | von Mangoldt function on $\mathcal{G}$ |
| $\bar{\Lambda}(m)$ | – | summatory function of $\Lambda(a)$ |
| $\Lambda^{\#}(y)$ | 3.1, 3.4, 3.8, 5.3 | generating function of $\bar{\Lambda}(m)$, $\Lambda(a)$ |
| $\omega(a)$ | 3.3, 4.1, 7.6, 7.7 | number of distinct prime divisors of $a$ |
| $\Omega(a)$ | 3.3, 4.1 | number of prime divisors of $a$, counting multiplicity |
| $\mathcal{G}^{\Omega}_{\text{even}}$, $\mathcal{G}^{\omega}_{\text{even}}$ | 4.1 | subsets of elements $a$ of $\mathcal{G}$ with $\Omega(a)$, $\omega(a)$ even, resp. |
| $\mathcal{G}^{\Omega}_{\text{odd}}$, $\mathcal{G}^{\omega}_{\text{odd}}$ | 4.1 | subsets of elements $a$ of $\mathcal{G}$ with $\Omega(a)$, $\omega(a)$ odd, resp. |
| $\mu(n)$ | – | classical Möbius function |
| $\mu(a)$ | 4.1, 6.5, 6.6, 7.4 | Möbius function on $\mathcal{G}$ |
| $\mu^{\#}(y)$, $M(y)$ | 2.2, 4.1, 6.5, 6.6 | generating function of $\mu(a)$ |

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

| *Notation* | *Section* | *Interpretation* |
|---|---|---|
| $\mu(n), \nu(n)$ | 8.1 | mean, variance of lengths of unordered factorization on $\mathcal{G}$, resp. |
| $\hat{\mu}(n), \hat{\nu}(n)$ | 8.1 | mean, variance of lengths of ordered factorization on $\mathcal{G}$, resp. |
| $\mu_D, \mu_\mathcal{F}, \mu_\mathcal{S}$ | 4.1 | Möbius functions on $D$, $\mathcal{F}$ $\mathcal{S}$ |
| $\lambda(a)$ | 4.1, 6.5, 6.6 | Liouville function on $\mathcal{G}$ |
| $(\Omega, \mathcal{F}, P)$ | 7.1 | probability space |
| $P(A)$ | 7.1, 7.6 | probability of $A$ in $\mathcal{F}$ |
| $X, X(\omega)$ | 7.1 | random variable on $(\Omega, \mathcal{F}, P)$ |
| $\mu(A)$ | 7.1 | distribution or law of a random variable |
| $EX$ | 7.1 | expectation (or mean) of random variable $X$ |
| $Var\, X$ | 7.1 | variance of random variable $X$ |
| $F * G$ | 7.1 | convolution of distribution functions $F$ and $G$ |
| $F_n \Rightarrow F$ | 7.1 | weak convergence of distribution functions |
| $\Phi(x)$ | 7.1 | the standard normal distribution function |
| $\mathcal{P}^*$ | 7.4 | subset of $\mathcal{P}$ |
| $\mathcal{S}(\mathcal{A}, \mathcal{P}^*, w)$ | 7.4 | sifting function |
| $\mathcal{S}(\mathcal{A}, \mathcal{P}^*, r)$ | 7.4 | sifting function |
| $f_r(a)$ | 7.5 | a truncation of $f(a)$ |
| $\nu(E)$ | 7.5 | additive set function of $E$ |
| $\nu_m(P(a,x,m))$ | 7.6 | number of true values of a proposition $P(a,x,m)$ among $a$ with $\partial(a) = m$ |
| $E \otimes F$ | 8.2 | direct factor decomposition |
| $M(B)$ | 8.3 | the subset of elements $bc$ with $b$ in given subset $B$ of $\mathcal{G}$ |
| $\delta(M(B))$ | 8.3 | the asymptotic density of $M(B)$ |
| $(\mathcal{G}, \sim, f_0)$ | 8.7 | additive arithmetical formation |

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

# INDEX

MARCEL DEKKER, INC.
270 Madison Avenue, New York, New York 10016

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016

Marcel Dekker, Inc.
270 Madison Avenue, New York, New York 10016