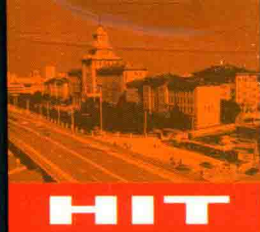


Analytic Number Theory —An Introductory Course



HIT

国外优秀数学著作
原版系列

解析数论入门教程

[美] 保罗·贝特曼 (Paul T. Bateman) [美] 哈罗德·戴默德 (Harold G. Diamond) 著



哈尔滨工业大学出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS



国外优秀数学著作
原版系列

Analytic Number Theory—An Introductory Course

解析数论入门教程

● [美] 保罗·贝特曼 (Paul T. Bateman)

● [美] 哈罗德·戴默德 (Harold G. Diamond)

· 著



哈尔滨工业大学出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

黑版贸审字 08-2017-095 号

Analytic Number Theory

An Introductory Course

by Paul T. Bateman and Harold G. Diamond

Copyright © 2004 by World Scientific Co. Pte. Ltd. All rights reserved. This book, or parts thereof, may not be reproduced in any form or by any means, electronic or mechanical, including photocopying, recording or any information storage and retrieval system now known or to be invented, without written permission from the Publisher.

Reprint edition arranged with World Scientific Co. Pte. Ltd., Singapore.

图书在版编目(CIP)数据

解析数论入门教程 = Analytic Number Theory: An Introductory Course: 英文/
(美)保罗·贝特曼(Paul T. Bateman), (美)哈罗德·戴默德(Harold G.
Diamond)著. —哈尔滨: 哈尔滨工业大学出版社, 2018. 1

ISBN 978-7-5603-6914-3

I. ①解… II. ①保… ②哈… III. ①数论-高等学校-教材-英文
IV. ①O156

中国版本图书馆 CIP 数据核字(2017)第 218848 号

策划编辑 刘培杰

责任编辑 张永芹 钱辰琛

封面设计 孙茵艾

出版发行 哈尔滨工业大学出版社

社 址 哈尔滨市南岗区复华四道街 10 号 邮编 150006

传 真 0451-86414749

网 址 <http://hitpress.hit.edu.cn>

印 刷 哈尔滨市工大节能印刷厂

开 本 787mm×1092mm 1/16 印张 24.5 字数 476 千字

版 次 2018 年 1 月第 1 版 2018 年 1 月第 1 次印刷

书 号 ISBN 978-7-5603-6914-3

定 价 78.00 元

(如因印装质量问题影响阅读, 我社负责调换)

To our wives, Felice and Nancy

Foreword

It is the goal of the series Monographs in Number Theory to publish research monographs and textbooks that provide clear expositions of various topics in number theory.

We are grateful to Professors Bateman and Diamond for agreeing to include their analytic number theory textbook as the first volume of the series.

We hope to continue to make available advanced monographs for researchers, as well as monographs and textbooks accessible to a broader audience, including undergraduate students, graduate students, and non-experts.

Bruce C. Berndt
Heng Huat Chan
Series Editors

Preface

Number theory holds a distinguished position in mathematics for its many results which are at once profound and yet easy to state. It is a beautiful subject, and we hope this book will invite students to its study.

Our theme is the use of analysis to treat multiplicative problems in number theory. We study several of the principal methods and results in this area, particularly those involving reasonably stable arithmetical entities. Typical examples include counts of integers having regularly occurring properties or summatory functions of arithmetic functions.

It seems paradoxical that analysis should be useful in number theory. The integers, the central objects of study in number theory, are the prototype of discreteness, while mathematical analysis, on the other hand, is concerned with continuous phenomena. Analysis is applied in two ways in this book: through direct real variable estimations, which we call "elementary" methods; and by using transforms, which put the apparatus of complex function theory at our disposal. Analysis serves both to establish results and to yield better understanding of the structure of problems.

This book is based on lecture notes we have given to generations of students in introductory graduate level courses on analytic number theory at the University of Illinois. We enjoyed teaching the material, and we hope that some of this enthusiasm comes through in our text.

A feature of our presentation is use of Riemann-Stieltjes integrals to unify and motivate arguments involving sums and integrals. We had previously hesitated to publish our notes out of a concern that some of the methodology might be unfamiliar to the intended audience. We are cautiously optimistic that now our formulation will be generally accepted. In

an appendix, we have presented the integration theory and a few further results that may be less well known; other background material is commonly taught in undergraduate courses in real analysis, complex analysis, and algebra or number theory.

Problems appear in the text near relevant techniques for their solution. They generally illustrate some point and give substance to theory; we encourage readers to consider them. The problems vary considerably in their difficulty.

Along with other writers, we suffer from a lack of symbols. For example, φ is used here for Euler's function as well as for various other functions. We generally identify each function in case of possible ambiguity. Also, usage of symbols is not always consistent among authors and topics. For instance, the number of distinct prime factors of an integer n is generally denoted by $\omega(n)$; in the chapters on sieves this symbol has another customary usage, so $\nu(n)$ serves to denote the number of distinct prime factors there. In the Symbol Index, we provide thumbnail sketches of symbols as a quick reminder to readers; these are not full definitions!

We are pleased to acknowledge the contributions of many people to this book. Most of our subject matter comes from the lectures and writings of distinguished number theorists (K. Chandrasekharan, H. Halberstam, A. E. Ingham, E. Landau, H. Rademacher, C. L. Siegel, and E. C. Titchmarsh, to name a few). Many students and colleagues over the years have provided stimulation, suggestions, and corrections to our original notes. We received help on parts of the manuscript from S. Ullom and from the referee for W.S.P. We are very appreciative of the assistance of F. Bateman, H. Halberstam, and J. Steinig for their many mathematical, grammatical, and typographic suggestions; and of A. J. Hildebrand for mathematical and L^AT_EX advice. We thank H. Britt for typing the manuscript.

Finally, we request readers to advise us of errors or obscurities that they find.

Urbana, Illinois

June, 2004

For this reprint we have made some minor corrections and updates and also added a few index items. Corrections and comments are maintained at the URL www.math.uiuc.edu/~diamond/ptbhgd/corrigenda.pdf.

October, 2008

Contents

Foreword	i
Preface	iii
Chapter 1 Introduction	1
1.1 Three problems	1
1.2 Asymmetric distribution of quadratic residues	1
1.3 The prime number theorem	2
1.4 Density of squarefree integers	3
1.5 The Riemann zeta function	8
1.6 Notes	11
Chapter 2 Calculus of Arithmetic Functions	13
2.1 Arithmetic functions and convolution	13
2.2 Inverses	17
2.3 Convergence	19
2.4 Exponential mapping	25
2.4.1 The 1 function as an exponential	28
2.4.2 Powers and roots	29
2.5 Multiplicative functions	31
2.6 Notes	38
Chapter 3 Summatory Functions	39
3.1 Generalities	39
3.2 Estimate of $Q(x) - 6x/\pi^2$	42
3.3 Riemann-Stieltjes integrals	44
3.4 Riemann-Stieltjes integrators	50

3.4.1	Convolution of integrators	52
3.4.2	Generalization of results on arithmetic functions	59
3.5	Stability	61
3.6	Dirichlet's hyperbola method	66
3.7	Notes	69
Chapter 4 The Distribution of Prime Numbers		71
4.1	General remarks	71
4.2	The Chebyshev ψ function	74
4.3	Mertens' estimates	78
4.4	Convergent sums over primes	81
4.5	A lower estimate for Euler's φ function	83
4.6	Notes	85
Chapter 5 An Elementary Proof of the P.N.T.		87
5.1	Selberg's formula	87
5.1.1	Features of Selberg's formula	90
5.2	Transformation of Selberg's formula	91
5.2.1	Calculus for R	92
5.3	Deduction of the P.N.T.	96
5.4	Propositions "equivalent" to the P.N.T.	98
5.5	Some consequences of the P.N.T.	105
5.6	Notes	107
Chapter 6 Dirichlet Series and Mellin Transforms		109
6.1	The use of transforms	109
6.2	Euler products	112
6.3	Convergence	116
6.3.1	Abscissa of convergence	118
6.3.2	Abscissa of absolute convergence	120
6.4	Uniform convergence	120
6.5	Analyticity	125
6.5.1	Analytic continuation	127
6.5.2	Continuation of zeta	128
6.5.3	Example of analyticity on $\sigma = \sigma_c$	129
6.6	Uniqueness	129
6.6.1	Identifying an arithmetic function	132
6.7	Operational calculus	133

6.8	Landau's oscillation theorem	137
6.9	Notes	140
Chapter 7 Inversion Formulas		141
7.1	The use of inversion formulas	141
7.2	The Wiener-Ikehara theorem	143
7.2.1	Example. Counting product representations	149
7.2.2	An O -estimate	151
7.3	A Wiener-Ikehara proof of the P.N.T.	151
7.4	A generalization of the Wiener-Ikehara theorem	154
7.5	The Perron formula	162
7.6	Proof of the Perron formula	164
7.7	Contour deformation in the Perron formula	168
7.7.1	The Fourier series of the sawtooth function	169
7.7.2	Bounded and uniform convergence	172
7.8	A "smoothed" Perron formula	173
7.9	Example. Estimation of $\sum T(1_2 * 1_3)$	176
7.10	Notes	180
Chapter 8 The Riemann Zeta Function		183
8.1	The functional equation	183
8.1.1	Justification of the interchange of \sum and \int	185
8.1.2	Symmetric form of the functional equation	186
8.2	O -estimates for zeta	187
8.3	Zeros of zeta	189
8.4	A zero-free region for zeta	192
8.5	An estimate of ζ'/ζ	197
8.6	Estimation of ψ	199
8.7	The P.N.T. with a remainder term	202
8.8	Estimation of M	208
8.9	The density of zeros in the critical strip	210
8.10	An explicit formula for ψ_1	213
8.11	Notes	219
Chapter 9 Primes in Arithmetic Progressions		221
9.1	Residue characters	221
9.2	Group structure of the coprime residue classes	225
9.3	Existence of enough characters	226

9.4	L functions	228
9.5	Proof of Dirichlet's theorem	231
9.6	P.N.T. for arithmetic progressions	233
9.7	Notes	236
Chapter 10 Applications of Characters		237
10.1	Integers generated by primes in residue classes	237
10.2	Sums of squares	242
10.3	A measure of nonprincipality	247
10.4	Quadratic excess	250
10.5	Evaluation of Gaussian sums	254
10.6	Notes	258
Chapter 11 Oscillation Theorems		261
11.1	Introduction	261
11.2	Approximate periodicity	262
11.3	The use of Landau's oscillation theorem	267
11.4	A quantitative estimate	269
11.5	The use of many singularities	272
11.5.1	Applications	277
11.6	Sign changes of $\pi(x) - \text{li } x$	278
11.7	The size of $M(x)/\sqrt{x}$	280
11.7.1	Numerical calculations	285
11.8	The error term in the divisor problem	286
11.9	Notes	287
Chapter 12 Sieves		289
12.1	Introduction	289
12.2	The sieve of Eratosthenes and Legendre	291
12.3	Sieve setup	293
12.4	The Brun-Hooley sieve	297
12.5	The large sieve	302
12.6	An extremal majorant	303
12.7	Proof of Theorem 12.9	309
12.8	Notes	312
Chapter 13 Application of Sieves		313
13.1	A Brun-Hooley estimate of twin primes	313

13.2	The Brun-Titchmarsh inequality	315
13.3	Primes represented by polynomials	319
13.4	A uniform two residue sieve estimate	325
13.5	Twin primes and Goldbach's problem	331
13.6	A heuristic formula for twin primes	334
13.7	Notes	337
Appendix A Results from Analysis and Algebra		339
A.1	Properties of real functions	339
A.1.1	Decomposition	339
A.1.2	Riemann-Stieltjes integrals	340
A.1.3	Integrators	342
A.2	The Euler gamma function	346
A.3	Poisson summation formula	347
A.4	Basis theorem for finite abelian groups	349
Bibliography		353
Index of Names and Topics		355
Index of Symbols		359

Chapter 1

Introduction

1.1 Three problems

The rational integers play an important role in many parts of analysis, e.g. as periods of functions such as $\sin 2\pi z$. In the other direction, one might try to apply analysis to establish properties of integers. Analytic number theory can be described as the study of problems concerning integers by use of methods from analysis. These problems are often easy to state; however, this is a poor guide for deciding how difficult they are to solve. Many innocent sounding arithmetical problems have not yet been solved or have been solved only by sophisticated methods.

We shall pose three problems here, each readily understood, and begin work upon the last one. Our approach is necessarily *ad hoc* at this stage, for we have available no general theory. The object here is to meet some ideas which will occur again. Also, it is interesting to see what we can do "from scratch." After some more machinery has been developed, the first two problems will be taken up and the third will be treated more efficiently and systematically.

1.2 Asymmetric distribution of quadratic residues

Let p be a prime number. In the sequel the symbols $p, p', \dots, p_1, p_2, \dots$ will be reserved for primes and $n, n', \dots, n_1, n_2, \dots$ for positive integers. We say that an integer n is a *quadratic residue modulo p* if $p \nmid n$ and n is congruent to some square modulo p . For the first few primes $p \equiv 3 \pmod{4}$ we list the least positive residues modulo p and underline the quadratic residues:

$p = 3$:	<u>1</u> 2
$p = 7$:	<u>1</u> <u>2</u> <u>3</u> <u>4</u> <u>5</u> 6
$p = 11$:	<u>1</u> <u>2</u> <u>3</u> <u>4</u> <u>5</u> <u>6</u> <u>7</u> <u>8</u> <u>9</u> 10
$p = 19$:	<u>1</u> <u>2</u> <u>3</u> <u>4</u> <u>5</u> <u>6</u> <u>7</u> <u>8</u> <u>9</u> 10 <u>11</u> 12 13 14 15 <u>16</u> <u>17</u> 18
$p = 23$:	<u>1</u> <u>2</u> <u>3</u> <u>4</u> <u>5</u> <u>6</u> <u>7</u> <u>8</u> <u>9</u> 10 11 <u>12</u> <u>13</u> 14 15 <u>16</u> <u>17</u> <u>18</u> 19 20 21 22

Table 1.1 QUADRATIC RESIDUES

This table suggests that, generally, residues occur near the beginning of each sequence and nonresidues occur near the end. We are led to conjecture

Theorem 1.1 *Let p be a prime, $p \equiv 3 \pmod{4}$. There are more quadratic residues modulo p between 0 and $p/2$ than between $p/2$ and p .*

This is a true theorem, and one obviously involving only integers. No “elementary” proof is presently known. This is not surprising, since the ordering of the least positive residues $r \equiv k^2 \pmod{p}$ is connected in a subtle way with the ordering of the integers $1 \leq k < p$. All known proofs involve such analytic tools as Fourier series or functions of a complex variable.

The above table suggests (and this is a familiar fact from elementary number theory) that if $p \equiv 3 \pmod{4}$ and n is a quadratic residue modulo p , then $p - n$ is not a quadratic residue and conversely. For primes $p \equiv 1 \pmod{4}$, Theorem 1.1 cannot hold, for in that case (again by elementary number theory) n is a quadratic residue precisely when $p - n$ is.

1.3 The prime number theorem

It has been known since the time of Euclid that there are infinitely many primes. (A proof of this fact is sketched in §1.5.) For $x \geq 1$, let $\pi(x)$ denote the number of primes in the interval $[1, x]$. Mathematicians have long sought exact formulas for $\pi(x)$ or for the n th prime number p_n . Around 1800 Gauss and Legendre independently conjectured

Theorem 1.2 (The prime number theorem).

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{x / \log x} = 1.$$

This theorem, which we shall call the P.N.T., is perhaps the most famous result in analytic number theory. Its proof withstood the best efforts of 19th century mathematicians until the end of the century, when proofs were discovered independently by J. Hadamard and C. J. de la Vallée Poussin.

Although this theorem deals ultimately with integers, it is perhaps less surprising that analysis plays a role here than in the first example. Indeed, the very statement of the theorem contains the notions of limit and logarithm, both of which belong to the domain of analysis.

1.4 Density of squarefree integers

A positive integer is said to be *squarefree* if it is not divisible by the square of any prime. We denote the squarefree integers by Q . The first few elements of Q are 1, 2, 3, 5, 6, 7, 10. We ask: What proportion of the positive integers are squarefree? This question is rather vague, and it can be made more precise as follows: We first define $Q(x)$ to be the number of squarefree integers not exceeding x . Next, we ask whether $Q(x)/x$ tends to a limit as x tends to ∞ , and finally what the value of this limit is, if it exists. In case the limit exists, it is called the (asymptotic) *density* of Q .

One can make a numerical experiment on a list of the positive integers by first deleting all multiples of 4, then all multiples of 9, then of 25, etc. The first operation leaves about $3/4$ of the integers. The second leaves about $8/9$ of those surviving the first operation, the third $24/25$, etc. We claim that divisibility by p^2 and divisibility by p'^2 ($p \neq p'$) are, in some sense, independent events (cf. the proof of Theorem 1.3, below, and §12.2).

The heuristic reasoning suggests that as $x \rightarrow \infty$,

$$\frac{Q(x)}{x} \rightarrow \lim_{n \rightarrow \infty} (1 - 2^{-2})(1 - 3^{-2}) \cdots (1 - p_n^{-2}) =: \prod_p (1 - p^{-2})$$

and numerical experiments reveal that

$$\frac{Q(10)}{10} = .7, \quad \frac{Q(100)}{100} = .61, \quad \frac{Q(1000)}{1000} = .608, \quad \frac{Q(10,000)}{10,000} = .6083.$$

We shall answer the question about the proportion of squarefree integers by the following three theorems.

Theorem 1.3 *The squarefree integers have the density*

$$\lim_{x \rightarrow \infty} Q(x)/x = \prod_p (1 - p^{-2}).$$

Theorem 1.4 (Euler product formula).

$$\prod_p (1 - p^{-2})^{-1} = \sum_{n=1}^{\infty} n^{-2}.$$

Theorem 1.5 $\left\{ \sum_{n=1}^{\infty} n^{-2} \right\}^{-1} = 6/\pi^2 = 0.607927 \dots$

Corollary 1.6 *The density of squarefree integers is $6/\pi^2$.*

Proof of Theorem 1.3. Let r be any nonnegative integer and for $x \geq 1$, let $Q^{(r)}(x)$ be the number of positive integers $n \leq x$ such that n is not divisible by the square of any of the first r primes. For example, $Q^{(0)}(x) = [x]$ and $Q^{(1)}(x) = [x] - [x/4]$. Here $[u]$ denotes the greatest integer not exceeding u . Clearly,

$$Q^{(0)}(x) \geq Q^{(1)}(x) \geq Q^{(2)}(x) \geq \dots \geq Q(x).$$

We shall first prove that if y is a multiple of $2^2 3^2 \dots p_r^2$, then

$$Q^{(r)}(y) = y(1 - 2^{-2})(1 - 3^{-2}) \dots (1 - p_r^{-2}).$$

An integer n is not divisible by the square of any of the first r primes precisely when n satisfies the simultaneous congruences

$$n \equiv a_i \pmod{p_i^2}, \quad 1 \leq i \leq r,$$

for an r -tuple of integers (a_1, \dots, a_r) with $0 < a_i < p_i^2$. For any fixed r -tuple (a_1, \dots, a_r) these simultaneous congruences have a unique solution among any $p_1^2 p_2^2 \dots p_r^2$ consecutive integers (Chinese remainder theorem). There are $(p_1^2 - 1)(p_2^2 - 1) \dots (p_r^2 - 1)$ r -tuples satisfying $0 < a_i < p_i^2$ for $1 \leq i \leq r$. Thus if a is a positive integer and $y = ap_1^2 \dots p_r^2$, then

$$Q^{(r)}(y) = a(p_1^2 - 1) \dots (p_r^2 - 1) = y(1 - p_1^{-2}) \dots (1 - p_r^{-2}).$$

Incidentally, this reasoning makes precise the sense in which we regard divisibility by p^2 and divisibility by p'^2 as independent events.

For arbitrary positive x let $y = [xp_1^{-2} \cdots p_r^{-2}] p_1^2 \cdots p_r^2$. We have

$$0 \leq Q^{(r)}(x) - Q^{(r)}(y) \leq x - y < p_1^2 p_2^2 \cdots p_r^2$$

and also

$$0 \leq (x - y) \prod_{\nu=1}^r (1 - p_\nu^{-2}) < x - y < p_1^2 p_2^2 \cdots p_r^2.$$

Thus

$$\begin{aligned} Q^{(r)}(x) &= x \prod_{\nu=1}^r (1 - p_\nu^{-2}) - (x - y) \prod_{\nu=1}^r (1 - p_\nu^{-2}) + Q^{(r)}(x) - Q^{(r)}(y) \\ &= x \prod_{\nu=1}^r (1 - p_\nu^{-2}) + \theta p_1^2 \cdots p_r^2, \end{aligned}$$

where θ is a number of modulus at most 1. Hence

$$\varliminf_{x \rightarrow \infty} \frac{Q(x)}{x} \leq \varliminf_{x \rightarrow \infty} \frac{Q^{(r)}(x)}{x} = \lim_{x \rightarrow \infty} \frac{Q^{(r)}(x)}{x} = \prod_{\nu=1}^r (1 - p_\nu^{-2}).$$

This inequality is valid for each r and thus

$$\varliminf_{x \rightarrow \infty} \frac{Q(x)}{x} \leq \prod_p (1 - p^{-2}),$$

where the product is interpreted as the limit of the preceding one as $r \rightarrow \infty$.

We next estimate $Q(x)$ from below. Let r be a positive integer. Then $Q^{(r)}(x) - Q(x)$ counts the number of integers $n \in [1, x]$ which contain no factor p^2 with $p \leq p_r$ and at least one factor p^2 for some $p > p_r$. Thus

$$\begin{aligned} Q^{(r)}(x) - Q(x) &\leq \#\{n \leq x : \exists \nu > r, p_\nu^2 \mid n\} \leq \sum_{\nu=r+1}^{\infty} \#\{n \leq x : p_\nu^2 \mid n\} \\ &= \sum_{\nu=r+1}^{\infty} \left[\frac{x}{p_\nu^2} \right] < \sum_{\nu=r+1}^{\infty} \frac{x}{\nu^2} < \int_r^{\infty} \frac{x}{t^2} dt = \frac{x}{r}, \end{aligned}$$

whence

$$\varliminf_{x \rightarrow \infty} \frac{Q(x)}{x} \geq \varliminf_{x \rightarrow \infty} \frac{Q^{(r)}(x)}{x} - \frac{1}{r} = \prod_{\nu=1}^r (1 - p_\nu^{-2}) - \frac{1}{r}.$$