Analytic Number Theory —An Introductory Course

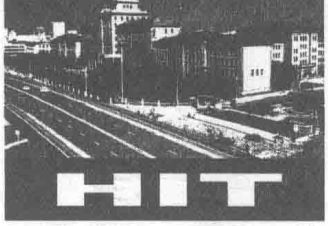
HIT

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

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS



国外优秀数学著作原版系列

解析数论入门教程

Analytic Number Theory—An Introductory Course

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

哈爾濱工業大學出版社
HARBIN INSTITUTE OF TECHNOLOGY PRESS

黑版贸审字 08-2017-095 号

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

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 LaTeX 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

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* $p, p', \ldots, p_1, p_2, \ldots$ *will be reserved for primes* and $n, n', \ldots, n_1, n_2, \ldots$ 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:

$p = 3$:	$\underline{1}\ 2$
$p = 7$:	$\underline{1}\ \underline{2}\ 3\ \underline{4}\ 5\ 6$
$p = 11$:	$\underline{1}\ 2\ \underline{3}\ \underline{4}\ \underline{5}\ 6\ 7\ 8\ \underline{9}\ 10$
$p = 19$:	$\underline{1}\ 2\ 3\ \underline{4}\ \underline{5}\ \underline{6}\ \underline{7}\ 8\ \underline{9}\ 10\ \underline{11}\ 12\ 13\ 14\ 15\ \underline{16}\ \underline{17}\ 18$
$p = 23$:	$\underline{1}\ \underline{2}\ \underline{3}\ \underline{4}\ 5\ \underline{6}\ 7\ \underline{8}\ \underline{9}\ 10\ 11\ \underline{12}\ \underline{13}\ 14\ 15\ \underline{16}\ 17\ \underline{18}\ 19\ 20\ 21\ 22$

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 nth prime number p_n. Around 1800 Gauss and Legendre independently conjectured

Theorem 1.2 (The prime number theorem).

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

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 $x \to \infty$,

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

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*

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

Theorem 1.4 (Euler product formula).

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

Theorem 1.5 $\{\sum_{n=1}^{\infty} n^{-2}\}^{-1} = 6/\pi^2 = 0.607927\ldots.$

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,

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

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

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

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

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

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

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

and also

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

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

$$\overline{\lim_{x\to\infty}}\frac{Q(x)}{x} \le \overline{\lim_{x\to\infty}}\frac{Q^{(r)}(x)}{x} = \lim_{x\to\infty}\frac{Q^{(r)}(x)}{x} = \prod_{\nu=1}^{r}(1-p_\nu^{-2}).$$

This inequality is valid for each r and thus

$$\overline{\lim_{x\to\infty}}\frac{Q(x)}{x} \le \prod_{p}(1-p^{-2}),$$

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

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 $p \le p_r$ and at least one factor p^2 for some $p > p_r$. Thus

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

whence

$$\underline{\lim_{x\to\infty}}\frac{Q(x)}{x} \ge \lim_{x\to\infty}\frac{Q^{(r)}(x)}{x} - \frac{1}{r} = \prod_{\nu=1}^{r}(1-p_\nu^{-2}) - \frac{1}{r}.$$