Hua Loo Keng

Introduction to Number Theory

Translated from the Chinese by Peter Shiu

With 14 Figures

Springer-Verlag
Berlin Heidelberg New York 1982

Hua Loo Keng

Institute of Mathematics
Academia Sinica
Beijing
The People's Republic of China

Peter Shiu

Department of Mathematics
University of Technology
Loughborough
Leicestershire LE 11 3 TU
United Kingdom

ISBN-13: 978-3-642-68132-5 e-ISBN-13: 978-3-642-68130-1
DOI: 10.1007/978-3-642-68130-1

Library of Congress Cataloging in Publication Data. Hua, Loo-Keng, 1910 –. Introduction to number theory. Translation of: Shu lun tao yin. Bibliography: p. Includes index. 1. Numbers, Theory of. I. Title. QA241.H7513.512'.7.82-645. ISBN-13:978-3-642-68132-5 (U.S.). AACR2

Softcover reprint of the hardcover 1st edition 1982

Typesetting: Buchdruckerei Dipl.-Ing. Schwarz' Erben KG, Zwettl.

2141/3140-5 4 3 2 1 0

Preface to the English Edition

The reasons for writing this book have already been given in the preface to the original edition and it suffices to append a few more points.

In the original edition I collected various recent results in number theory and put them in a text book suitable for teaching purposes. The book contains: The elementary proof of the prime number theorem due to Selberg and Erdős; Roth's theorem; A. O. Gelfond's solution to Hilbert's seventh problem; Siegel's theorem on the class number of binary quadratic forms; Linnik's proof of the Hilbert-Waring theorem; Selberg's sieve method and Schnirelman's theorem on the Goldbach problem; Vinogradov's result concerning least quadratic non-residues. It also contains some of my own results, for example, on the estimation of complete trigonometric sums, on least primitive roots, and on the Prouhet-Tarry problem. The reader can see that the book is much influenced by the work of Landau, Hardy, Mordell, Davenport, Vinogradov, Erdős and Mahler. In the quarter of a century between the two editions of the book there have been, of course, many new and exciting developments in number theory, and I am grateful to Professor Wang Yuan for incorporating many new results which will guide the reader to the literature concerning the latest developments.

It has been doubtful in the past whether number theory is a "useful" branch of mathematics. It is futile to get too involved in the argument but it may be relevant to point out some specific examples of applications. The fundamental principle behind the *Public Key Code* is the following: It is not difficult to construct a large prime number but it is not easy to factorize a large composite integer. For example, it only takes 45 seconds computing time to find the first prime exceeding 2^{200} (namely $2^{200} + 235$, a number with 61 digits), but the computing time required to factorize a product of two primes, each with 61 digits, exceeds 4 million million years. According to Fermat's theorem: if p is prime then $a^{p-1} \equiv 1 \pmod{p}$, and if n is composite then $a^{\phi(n)} \equiv 1 \pmod{n}$, $\phi(n) < n - 1$. The determination of whether n is prime by this method is quite fast and this is included in the book. Next the location of the zeros of the Riemann Zeta function is a problem in pure mathematics. However, an interesting problem emerged during calculations of these zeros: Can mathematicians always rely on the results obtained from computing machines, and if there are mistakes in the machines how do we find out? Generally speaking calculations by machines have to be accepted by faith. For this reason Rosser, Schoenfeld and Yohe were particularly careful when they used computers to calculate the zeros of the Riemann Zeta function. In their critical examination of the program they discovered that there were several logical errors in the machine itself. The machine has been in use for some years and no-one had found these errors until the three mathematicians wanted to scrutinize the results on a problem which has no practical applications. Apart from these there are applications from algebraic number theory and from the theory of rational approximations to real numbers which we need not mention.

Finally I must point out that this English edition owes its existence to Professor Heini Halberstam for suggesting it, to Dr. Peter Shiu for translating it and to Springer-Verlag for publishing it. I am particularly grateful to Peter Shiu for his excellent translation and to Springer-Verlag for their beautiful printing.

March 1981, Beijing Hua Loo-Keng

Preface to the Original Edition

This preface has been revised more than once. The reason is that, during the last fifteen years, the author's knowledge of mathematics has changed and the needs of the readers are different. Moreover the content of the book has been so expanded during this period that the old preface has become quite unsuitable.

Everything is still very clear in my memory. The plan for the book was conceived round about 1940 when I first lectured on number theory at Kwang Ming University. I had written some 85 thousand words (characters) for the first draft and I estimated that another 25 thousand words were needed to complete the manuscript. But where was I to publish the work? I therefore could not summon up the energy required to complete the project. Later when lecturing in America I made additions and revisions to the manuscripts, but these were made for my teaching requirements and not with a view to publishing the book.

The real effort required for the task was given after the liberation. Since our country has very few reference books there is need for a broad introductory text in number theory. It seems a little peculiar that, even though we have been busier after the liberation, with the help of comrades the project actually has progressed faster. The book has also increased in size with the addition of new chapters and the incorporation of recent results which are within its scope.

Apart from giving a broad introduction to number theory and some of its fundamental principles the author has also tried to emphasize several points to its readers.

First there is a close relationship between number theory and mathematics as a whole. In the history of mathematics we often see the various problems, methods and concepts in number theory having a significant influence on the progress of mathematics. On the other hand there are also frequent instances of applying the methods and results of the other branches of mathematics to solve concrete problems in number theory. However it is often not easy to see this relationship in many existing introductory books. Indeed many "self-contained" books for beginners in number theory give an erroneous impression to their readers that number theory is an isolated and independent branch of mathematics. In this book the author tries to highlight this relationship within the scope of elementary number theory. For example: the relationship between the prime number theorem and Fourier series (the limitation on the nature of the book does not allow us to describe the relationship between the prime number theorem and integral functions); the partition problem, the four squares problem and their relationship to modular functions, the theory of quadratic forms, modular transformations and their relationship to Lobachevskian geometry etc.

Secondly an important progression in mathematics is the development of abstract concepts from concrete examples. Specific concrete examples are often the basis of abstract notions and the methods employed on the examples are frequently the source of deep and powerful techniques in advanced mathematics. One cannot go very far by merely learning bare definitions and methods from abstract notions without knowing the source of the definitions in the concrete situation. Indeed such an approach may lead to insurmountable difficulties later in research situations. The history of mathematics is full of examples in which whole subjects were developed from methods employed to tackle practical problems, for example, in mechanics and in physics. As for mathematics itself the most fundamental notions are "numbers" and "shapes". From "shapes" we have geometric intuition and from "numbers" we have arithmetic operations which are rich sources for mathematics. In this book the author tries to bring out the concrete examples underlying the abstract notions hoping that the readers may remember them when they make further advances in mathematics. For example, in Chapter 4 and Chapter 14, concrete examples are given to illustrate abstract algebra; indeed the example on finite fields describes the situation of general finite fields.

Thirdly, for beginners engaging in research, a most difficult feature to grasp is that of quality – that is the depth of a problem. Sometimes authors work courageously and at length to arrive at results which they believe to be significant and which experts consider to be shallow. This can be explained by the analogy of playing chess. A master player can dispose of a beginner with ease no matter how hard the latter tries. The reason is that, even though the beginner may have planned a good number of moves ahead, by playing often the master has met many similar and deeper problems; he has read standard works on various aspects of the game so that he can recall many deeply analyzed positions. This is the same in mathematical research. We have to play often with the masters (that is, try to improve on the results of famous mathematicians); we must learn the standard works of the game (that is, the "well-known" results). If we continue like this our progress becomes inevitable. This book attempts to direct the reader to work in this way. Although the nature of the book excludes the very deep results in number theory the author introduces different methods with varying depths. For example, in the estimation of the partition function $p(n)$, the simplest of algebraic methods is used first to get a rough estimate, then using a slightly deeper method the asymptotic formula for $\log p(n)$ is obtained. It is also indicated how an asymptotic formula for $p(n)$ can be obtained by a Tauberian method and how an asymptotic expansion for $p(n)$ can be obtained using results in advanced modular function theory and methods in analytic number theory. It is then easy to judge the various levels of depth in the methods used by following the successive improvement of results.

The book is not written for a university course; its content far exceeds the syllabus for a single course in number theory. However lecturers can use it as a course text by taking Chapters 1 – 6 together with a suitable selection from the other chapters. Actually the book does not demand much previous knowledge in mathematics. Second year university students could understand most of the book, and those who know advanced calculus could understand the whole book apart from Sections 9.2, 12.14, 12.15 and 17.9 where some knowledge of complex functions theory is required. Those studying by themselves should not find any special difficulties either.

I am eternally grateful to the following comrades: Yue Min Yi, Wang Yuan, Wu Fang, Yan Shi Jian, Wei Dao Zheng, Xu Kong Shi and Ren Jian Hua. Since 1953, when I began my lectures, they have continually given me suggestions, and sometimes even offer to help with the revision. They have also assisted me throughout the stages of publication, particularly comrade Yue Min Yi. I would also like to thank Professor Zhang Yuan Da for his valuable suggestion on a method of preparing the manuscript for the typesetter.

Although we have collectively laboured over the book it must still contain many mistakes. I should be grateful if readers would inform me of these, whether they are misprints, errors in content, or other suggestions. There is much material that appears here for the first time in a book, as well as some unpublished research material, so that there must be plenty of room for improvement. Concerning this point we invite the readers for their valuable contributions.

September 1956, Beijing Hua Loo-Keng

Table of Contents

List of Frequently Used Symbols

$[\alpha]$ = the greatest integer not exceeding α.
$\{\alpha\} = \alpha - [\alpha]$ = the fractional part of α.
$\langle\alpha\rangle$ = the distance of α from the nearest integer, that is $\min(\alpha - [\alpha], [\alpha] + 1 - \alpha)$.
$(a, b, \ldots, c)$ = the greatest common divisor of $a, b, \ldots, c$.
$[a, b, \ldots, c]$ = the least common multiple of $a, b, \ldots, c$.
$a|b$ means a divides b.
$a \nmid b$ means a does not divide b.
$p^u \| a$ means $p^u | a$ and $p^{u+1} \nmid a$.
$a \equiv b \pmod{m}$ means $m | a - b$.
$a \not\equiv b \pmod{m}$ means $m \nmid a - b$.
$\prod_{d|m}$ and $\sum_{d|m}$ denote the product and the sum over the divisors d of m.
$\left(\frac{n}{p}\right)$ is Legendre's symbol; see §3.1.
$\left(\frac{n}{m}\right)$ is Jacobi's symbol; see §3.6.
$\left(\frac{d}{m}\right)$ where d is not a perfect square, $d \equiv 0$ or $1 \pmod 4$ and $m > 0$, is Kronecker's symbol; see §12.3.
$\operatorname{ind} n$ denotes the index of n; see §3.8.
$\partial^0 f$ denotes the degree of the polynomial $f(x)$.
$\ll$, O, o, $\sim$ see §5.1.
$\omega(n)$ denotes the number of distinct prime divisors of n.
$\Omega(n)$ denotes the total number of prime divisors of n.
$\max(a, b, \ldots, c)$ denotes the greatest number among $a, b, \ldots, c$.
$\min(a, b, \ldots, c)$ denotes the least number among $a, b, \ldots, c$.
$\Re s$ denotes the real part of the complex number s.
γ denotes Euler's constant.
$\{a, b, c\}$ represents the quadratic form $ax^2 + bxy + cy^2$; see §12.1.
(z_1, z_2, z_3, z_4) denotes the cross ratio of the four points z_1, z_2, z_3, z_4; see §13.3.
$A \stackrel{L}{=} B$ means that the matrices A and B are left associated.
$N(\mathfrak{M})$ denotes the norm of $\mathfrak{M}$; see §14.9.
$\{a_n\}$ denotes the sequence $a_1, a_2, \ldots$.
$\sim$ is an equivalence sign; see §12.1, §13.6, §14.5 and §16.12.

$[a_0, a_1, \ldots, a_N]$ or $a_0 + \frac{1}{a_1 +}\, \frac{1}{a_2 +} \cdots \frac{1}{+ a_N}$ denotes a finite continued fraction;

$p_n/q_n = [a_0, a_1, \ldots, a_n]$ is the n-th convergent of a continued fraction.

$S(\alpha) = \alpha^{(1)} + \alpha^{(2)} + \cdots + \alpha^{(n)}$ is the trace of α.

$N(\alpha) = \alpha^{(1)}\alpha^{(2)} \cdots \alpha^{(n)}$ is the norm of α.

$\Delta(\alpha_1, \ldots, \alpha_n)$ denotes the discriminant of $\alpha_1, \ldots, \alpha_n$; $\Delta = \Delta(R(\vartheta))$ denotes the discriminant of the integral basis for $R(\vartheta)$. See §16.3 and §16.4.

$\varphi(m)$ is Euler's function; see §2.3.

$\operatorname{li} x$ see §5.2.

$\pi(x)$ see §5.3.

$\mu(m)$ see §6.1.

$d(n)$ see §6.1.

$\sigma(n)$ see §6.1.

$\Lambda(n)$ see §6.1.

$\Lambda_1(n)$ see §6.1.

$\chi(n)$ see §7.2.

$p(n)$ see §8.2.

$\vartheta(n)$ see §9.1.

$\psi(n)$ see §9.1.

$g(k)$ see §18.1.

$G(k)$ see §18.1.

$v(k)$ see §18.5.

$N(k)$ see §18.6.

$M(k)$ see §18.6.

$\zeta(s) = \sum_{n=1}^{\infty} 1/n^s$ is the Riemann Zeta function.

$e(f(x)) = e^{2\pi i f(x)}$, $e_q(f(x)) = e^{2\pi i f(x)/q}$.

$S(a, \chi) = \sum_{n=1}^{m} \chi(n) e^{2\pi i a n/m}$ is a character sum.

$\tau(\chi) = S(1, \chi)$.

$S(n, m) = \sum_{x=0}^{m-1} e^{2\pi i n x^2/m}$, $(n, m) = 1$, is a Gauss sum.

$S(q, f(x)) = \sum_{x=0}^{q-1} e_q(f(x))$.