An Introduction To Sieve Methods And Their Applications

To Number Theory Translated from the Chinese by Peter Shiu With 14 Figures Springer-Verlag Berlin Heidelberg New York 1982 HuaLooKeng Institute of Mathematics Academia Sinica Beijing The People's Republic of China PeterShlu 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 DOl: 10.1007/978-3-642-68130-1 Library of Congress Cataloging in Publication Data. Hua, Loo-Keng, 1910 -. Introduc tion to number theory. Translation of: Shu lun tao yin. Bibliography: p. Includes index. 1. Numbers, Theory of. I. Title. QA241.H7513.5 12'.7.82-645. ISBN-13:978-3-642-68132-5 (U.S.). AACR2 This work is subject to copyright. All rights are reserved, whether the whole or part of the material is concerned, specifically those of translation, reprinting, reuse of illustra tions, broadcasting, reproductiOli by photocopying machine or similar means, and storage in data banks. Under {sect} 54 of the German Copyright Law where copies are made for other than private use a fee is payable to "VerwertungsgeselIschaft Wort", Munich. © Springer-Verlag Berlin Heidelberg 1982 Softcover reprint of the hardcover 1st edition 1982 Typesetting: Buchdruckerei Dipl.-Ing. Schwarz' Erben KG, Zwettl. 214113140-5432 I 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

This is a true masterpiece that will prove to be indispensable to the serious researcher for many years to come. --Enrico Bombieri, Institute for Advanced Study This is a truly comprehensive account of sieves and their applications, by two of the world's greatest authorities. Beginners will find a thorough introduction to the subject, with plenty of helpful motivation. The more practised reader will appreciate the authors' insights into some of the more mysterious parts of the theory, as well as the wealth of new examples. --Roger Heath-Brown, University of Oxford, Fellow of Royal Society This is a comprehensive and up-to-date treatment of sieve methods. The theory of the sieve is developed thoroughly with complete and accessible proofs of the basic theorems. Included is a wide range of applications, both to traditional questions such as those concerning primes, and to areas previously unexplored by sieve methods, such as elliptic curves, points on cubic surfaces and quantum ergodicity. New proofs are given also of some of the central theorems of analytic number theory; these proofs emphasize and take advantage of the applicability of sieve ideas. The book contains numerous comments which provide the reader with insight into the workings of the subject, both as to what the sieve can do and what it cannot do. The authors reveal recent developements by which the parity barrier can be breached, exposing golden nuggets of the subject, previously inaccessible. The variety in the topics covered and in the levels of difficulty encountered makes this a work of value to novices and experts alike, both as an educational tool and a basic reference.

Developed from the author's popular text, A Concise Introduction to the Theory of Numbers, this book provides a comprehensive initiation to all the major branches of number theory. Beginning with the rudiments of the subject, the author proceeds to more advanced topics, including elements of cryptography and primality testing, an account of number fields in the classical vein including properties of their units, ideals and ideal classes, aspects of analytic number theory including studies of the Riemann zeta-function, the prime-number theorem and primes in arithmetical progressions, a description of the Hardy–Littlewood and sieve methods from respectively additive and multiplicative number theory and an exposition of the arithmetic of elliptic curves. The book includes many worked examples, exercises and further reading. Its wider coverage and versatility make this book suitable for courses extending from the elementary to beginning graduate studies.

An Introduction to Sieve Methods and Their ApplicationsCambridge University Press

How can you tell whether a number is prime? What if the number has hundreds or thousands of digits? This question may seem abstract or irrelevant, but in fact, primality tests are performed every time we make a secure online transaction. In 2002, Agrawal, Kayal, and Saxena answered a long-standing open question in this context by presenting a deterministic test (the AKS algorithm) with polynomial running time that checks whether a number is prime or not. What is more, their methods are essentially elementary, providing us with a unique opportunity to give a complete explanation of a current mathematical breakthrough to a wide audience. Rempe-Gillen and Waldecker introduce the aspects of number theory, algorithm theory, and cryptography that are relevant for the AKS algorithm and explain in detail why and how this test works. This book is specifically designed to make the reader familiar with the background that is necessary to appreciate the AKS algorithm and begins at a level that is suitable for secondary school students, teachers, and interested amateurs. Throughout the book, the reader becomes involved in the topic by means of numerous exercises.

Praise for the Second Edition: "The authors present an intuitive and easy-to-read book. ... accompanied by many examples, proposed exercises, good references, and comprehensive appendices that initiate the reader unfamiliar with MATLAB." —Adolfo Alvarez Pinto, International Statistical Review "Practitioners of EDA who use MATLAB will want a copy of this book. ... The authors have done a great service by bringing together so many EDA routines, but their main accomplishment in this dynamic text is providing the understanding and tools to do EDA. —David A Huckaby, MAA Reviews Exploratory Data Analysis (EDA) is an important part of the data analysis process. The methods presented in this text are ones that should be in the toolkit of every data scientist. As computational sophistication has increased and data sets have grown in size and complexity, EDA has become an even more important process for visualizing and summarizing data before making assumptions to generate hypotheses and models. Exploratory Data Analysis with MATLAB, Third Edition presents EDA methods from a computational perspective and uses numerous examples and applications to show how the methods are used in practice. The authors use MATLAB code, pseudo-code, and algorithm descriptions to illustrate the concepts. The MATLAB code for examples, data sets, and the EDA Toolbox are available for download on the book’s website. New to the Third Edition Random projections and estimating local intrinsic dimensionality Deep learning autoencoders and stochastic neighbor embedding Minimum spanning tree and additional cluster validity indices Kernel density estimation Plots for visualizing data distributions, such as beanplots and violin plots A chapter on visualizing categorical data

The last one hundred years have seen many important achievements in the classical part of number theory. After the proof of the Prime Number Theorem in 1896, a quick development of analytical tools led to the invention of various new methods, like Brun's sieve method and the circle method of Hardy, Littlewood and Ramanujan; developments in topics such as prime and additive number theory, and the solution of Fermat’s problem. Rational Number Theory in the 20th Century: From PNT to FLT offers a short survey of 20th century developments in classical number theory, documenting between the proof of the Prime Number Theorem and the proof of Fermat's Last Theorem. The focus lays upon the part of number theory that deals with properties of integers and rational numbers. Chapters are divided into five time periods, which are then further divided into subject areas. With

the introduction of each new topic, developments are followed through to the present day. This book will appeal to graduate researchers and student in number theory, however the presentation of main results without technicalities will make this accessible to anyone with an interest in the area.

This book has grown out of a course of lectures I have given at the Eidgenossische Technische Hochschule, Zurich. Notes of those lectures, prepared for the most part by assistants, have appeared in German. This book follows the same general plan as those notes, though in style, and in text (for instance, Chapters III, V, VIII), and in attention to detail, it is rather different. Its purpose is to introduce the non-specialist to some of the fundamental results in the theory of numbers, to show how analytical methods of proof fit into the theory, and to prepare the ground for a subsequent inquiry into deeper questions. It is pub lished in this series because of the interest evinced by Professor Beno Eckmann. I have to acknowledge my indebtedness to Professor Carl Ludwig Siegel, who has read the book, both in manuscript and in print, and made a number of valuable criticisms and suggestions. Professor Raghavan Narasimhan has helped me, time and again, with illuminating comments. Dr. Harold Diamond has read the proofs, and helped me to remove obscurities. I have to thank them all. K.C.

Exploring one of the most dynamic areas of mathematics, Advanced Number Theory with Applications covers a wide range of algebraic, analytic, combinatorial, cryptographic, and geometric aspects of number theory. Written by a recognized leader in algebra and number theory, the book includes a page reference for every citing in the bibliography and mo

This book surveys the current state of the "small" sieve methods developed by Brun, Selberg and later workers. The book is suitable for university graduates making their first acquaintance with the subject, leading them towards the frontiers of modern research and unsolved problems in the subject area.

This valuable reference addresses the methods leading to contemporary developments in number theory and coding theory, originally presented as lectures at a summer school held at Bilkent University, Ankara, Turkey.

Advanced Methods in Molecular Biology and Biotechnology: A Practical Lab Manual is a concise reference on common protocols and techniques for advanced molecular biology and biotechnology experimentation. Each chapter focuses on a different method, providing an overview before delving deeper into the procedure in a step-by-step approach. Techniques covered include genomic DNA extraction using cetyl trimethylammonium bromide (CTAB) and chloroform extraction, chromatographic techniques, ELISA, hybridization, gel electrophoresis, dot blot analysis and methods for studying polymerase chain reactions. Laboratory protocols and standard operating procedures for key equipment are also discussed, providing an instructive overview for lab work. This practical guide focuses on the latest advances and innovations in methods for molecular biology and biotechnology investigation, helping researchers and practitioners enhance and advance their own methodologies and take their work to the next level. Explores a wide range of advanced methods that can be applied by researchers in molecular biology and biotechnology Features clear, step-by-step instruction for applying the techniques covered Offers an introduction to laboratory protocols and recommendations for best practice when conducting experimental work, including standard operating procedures for key equipment

This book seeks to describe the rapid development in recent decades of sieve methods able to detect prime numbers. The subject began with Eratosthenes in antiquity, took on new shape with Legendre's form of the sieve, was substantially reworked by Ivan M. Vinogradov and Yuri V. Linnik, but came into its own with Robert C. Vaughan and important contributions from others, notably Roger Heath-Brown and Henryk Iwaniec. Prime-Detecting Sieves breaks new ground by bringing together several different types of problems that have been tackled with modern sieve methods and by discussing the ideas common to each, in particular the use of Type I and Type II information. No other book has undertaken such a systematic treatment of prime-detecting sieves. Among the many topics Glyn Harman covers are primes in short intervals, the greatest prime factor of the sequence of shifted primes, Goldbach numbers in short intervals, the distribution of Gaussian primes, and the recent work of John Friedlander and Iwaniec on primes that are a sum of a square and a fourth power, and Heath-Brown's work on primes represented as a cube plus twice a cube. This book contains much that is accessible to beginning graduate students, yet also provides insights that will benefit established researchers.

This is a self-contained introduction to analytic methods in number theory, assuming on the part of the reader only what is typically learned in a standard undergraduate degree course. It offers to students and those beginning research a systematic and consistent account of the subject but will also be a convenient resource and reference for more experienced mathematicians. These aspects are aided by the inclusion at the end of each chapter a section of bibliographic notes and detailed exercises.

This text by a noted pair of experts is regarded as the definitive work on sieve methods. It formulates the general sieve problem, explores the theoretical background, and illustrates significant applications. 1974 edition.

Combinatorial enumeration is a readily accessible subject full of easily stated, but sometimes tantalizingly difficult problems. This book leads the reader in a leisurely way from basic notions of combinatorial enumeration to a variety of topics, ranging from algebra to statistical physics. The book is organized in three parts: Basics, Methods, and Topics. The aim is to introduce readers to a fascinating field, and to offer a sophisticated source of information for professional mathematicians desiring to learn more. There are 666 exercises, and every chapter ends with a highlight section, discussing in detail a particularly beautiful or famous result.

Prime numbers have fascinated mathematicians since the time of Euclid. This book presents some of our best tools to capture the properties of these fundamental objects, beginning with the most basic notions of asymptotic estimates and arriving at the forefront of mathematical research. Detailed proofs of the recent spectacular advances on small and large gaps between primes are made accessible for the first time in textbook form. Some other highlights include an introduction to probabilistic methods, a detailed study of sieves, and elements of the theory of pretentious multiplicative functions leading to a proof of Linnik's theorem. Throughout, the emphasis has been placed on explaining the main ideas rather than the most general results available. As a result, several methods are presented in terms of concrete examples that simplify technical details, and theorems are stated in a form that facilitates the understanding of their proof at the cost of sacrificing some generality. Each chapter concludes with numerous exercises of various levels of difficulty aimed to exemplify the material, as well as to expose the readers to more advanced topics and point them to further reading sources.

Analytic Number Theory distinguishes itself by the variety of tools it uses to establish results. One of the primary attractions of this theory is its vast diversity of concepts and methods. The main goals of this book are to show the scope of the theory, both in classical and modern directions, and to exhibit its wealth and prospects, beautiful theorems, and powerful techniques. The book is written with graduate students in mind, and the authors nicely balance clarity, completeness, and generality. The exercises in each section serve dual purposes, some intended to improve readers' understanding of the subject and others providing additional information. Formal prerequisites for the major part of the book do not go beyond calculus, complex analysis, integration, and Fourier series and integrals. In later chapters automorphic forms

become important, with much of the necessary information about them included in two survey chapters.
Nearly a hundred years have passed since Viggo Brun invented his famous sieve, and the use of sieve methods is constantly evolving. As probability and combinatorics have penetrated the fabric of mathematical activity, sieve methods have become more versatile and sophisticated and in recent years have played a part in some of the most spectacular mathematical discoveries. Many arithmetical investigations encounter a combinatorial problem that requires a sieving argument, and this tract offers a modern and reliable guide in such situations. The theory of higher dimensional sieves is thoroughly explored, and examples are provided throughout. A Mathematica® software package for sieve-theoretical calculations is provided on the authors' website. To further benefit readers, the Appendix describes methods for computing sieve functions. These methods are generally applicable to the computation of other functions used in analytic number theory. The appendix also illustrates features of Mathematica® which aid in the computation of such functions.
[Hilbert's] style has not the terseness of many of our modem authors in mathematics, which is based on the assumption that printer's labor and paper are costly but the reader's effort and time are not. H. Weyl [143] The purpose of this book is to describe the classical problems in additive number theory and to introduce the circle method and the sieve method, which are the basic analytical and combinatorial tools used to attack these problems. This book is intended for students who want to lel?Ill additive number theory, not for experts who already know it. For this reason, proofs include many "unnecessary" and "obvious" steps; this is by design. The archetypical theorem in additive number theory is due to Lagrange: Every nonnegative integer is the sum of four squares. In general, the set A of nonnegative integers is called an additive basis of order h if every nonnegative integer can be written as the sum of h not necessarily distinct elements of A. Lagrange 's theorem is the statement that the squares are a basis of order four. The set A is called a basis offinite order if A is a basis of order h for some positive integer h. Additive number theory is in large part the study of bases of finite order. The classical bases are the squares, cubes, and higher powers; the polygonal numbers; and the prime numbers. The classical questions associated with these bases are Waring's problem and the Goldbach conjecture.
A 2006 text based on courses taught successfully over many years at Michigan, Imperial College and Pennsylvania State.
This book is intended for use in a rigorous introductory PhD level course in econometrics.
Number theory is one of the few areas of mathematics where problems of substantial interest can be fully described to someone with minimal mathematical background. Solving such problems sometimes requires difficult and deep methods. But this is not a universal phenomenon; many engaging problems can be successfully attacked with little more than one's mathematical bare hands. In this case one says that the problem can be solved in an elementary way. Such elementary methods and the problems to which they apply are the subject of this book. Not Always Buried Deep is designed to be read and enjoyed by those who wish to explore elementary methods in modern number theory. The heart of the book is a thorough introduction to elementary prime number theory, including Dirichlet's theorem on primes in arithmetic progressions, the Brun sieve, and the Erdos-Selberg proof of the prime number theorem. Rather than trying to present a comprehensive treatise, Pollack focuses on topics that are particularly attractive and accessible. Other topics covered include Gauss's theory of cyclotomy and its applications to rational reciprocity laws, Hilbert's solution to Waring's problem, and modern work on perfect numbers. The nature of the material means that little is required in terms of prerequisites: The reader is expected to have prior familiarity with number theory at the level of an undergraduate course and a first course in modern algebra (covering groups, rings, and fields). The exposition is complemented by over 200 exercises and 400 references.
"This book is the first volume of a two-volume textbook for undergraduates and is indeed the crystallization of a course offered by the author at the California Institute of Technology to undergraduates without any previous knowledge of number theory. For this reason, the book starts with the most elementary properties of the natural integers. Nevertheless, the text succeeds in presenting an enormous amount of material in little more than 300 pages."-—MATHEMATICAL REVIEWS
A description of 148 algorithms fundamental to number-theoretic computations, in particular for computations related to algebraic number theory, elliptic curves, primality testing and factoring. The first seven chapters guide readers to the heart of current research in computational algebraic number theory, including recent algorithms for computing class groups and units, as well as elliptic curve computations, while the last three chapters survey factoring and primality testing methods, including a detailed description of the number field sieve algorithm. The whole is rounded off with a description of available computer packages and some useful tables, backed by numerous exercises. Written by an authority in the field, and one with great practical and teaching experience, this is certain to become the standard and indispensable reference on the subject.
"Richard Stanley's two-volume basic introduction to enumerative combinatorics has become the standard guide to the topic for students and experts alike. This thoroughly revised second edition of Volume 1 includes ten new sections and more than 300 new exercises, most with solutions, reflecting numerous new developments since the publication of the first edition in 1986. The author brings the coverage up to date and includes a wide variety of additional applications and examples, as well as updated and expanded chapter bibliographies. Many of the less difficult new exercises have no solutions so that they can more easily be assigned to students. The material on P-partitions has been rearranged and generalized; the treatment of permutation statistics has been greatly enlarged; and there are also new sections on q-analogues of permutations, hyperplane arrangements, the cd-index, promotion and evacuation and differential posets"--
"In order to become proficient in mathematics, or in any subject," writes Andre Weil, "the student must realize that most topics in volve only a small number of basic ideas. " After learning these basic concepts and theorems, the student should "drill in routine exercises, by which the necessary reflexes in handling such concepts may be ac quired. . . . There can be no real understanding of the basic concepts of a mathematical theory without an ability to use them intelligently and apply them to specific problems. " Weil's insightfulobservation becomes especially important at the graduate and research level. It is the viewpoint of this book. Our goal is to acquaint the student with the methods of analytic number theory as rapidly as possible through examples and exercises. Any landmark theorem opens up a method of attacking other problems. Unless the student is able to sift out from the mass of theory the underlying techniques, his or her understanding will only be academic and not that of a participant in research. The prime number theorem has given rise to the rich Tauberian theory and a general method of Dirichlet series with which one can study the asymptotics of sequences. It has also motivated the development of sieve methods. We focus on this theme in the book. We also touch upon the emerging Selberg theory (in Chapter 8) and p-adic analytic number theory (in Chapter 10).
One notable new direction this century in the study of primes has been the influx of ideas from probability. The goal of this book is to provide insights into the prime numbers and to describe how a sequence so tautly determined can incorporate such a striking amount of randomness. The book opens with some classic topics of number theory. It ends with a discussion of some of the outstanding conjectures in number theory. In between are an excellent chapter on the stochastic properties of primes and a walk through an elementary proof of the Prime Number Theorem. This book is suitable for anyone who has had a little number theory and some advanced calculus involving estimates. Its engaging style and invigorating point of view will make refreshing reading for advanced undergraduates through research mathematicians.
Superb introduction to Euclidean algorithm and its consequences, congruences, continued fractions, powers of an integer modulo m, Gaussian integers, Diophantine equations, more. Problems, with answers. Bibliography.
This text originated as a lecture delivered November 20, 1984, at Queen's University, in the undergraduate colloquium senes. In another colloquium lecture, my colleague Morris Orzech, who had consulted the latest edition of the Guinness Book of Records, reminded me very

gently that the most "innumerate" people of the world are of a certain trible in Mato Grosso, Brazil. They do not even have a word to express the number "two" or the concept of plurality. "Yes, Morris, I'm from Brazil, but my book will contain numbers different from ·one.'" He added that the most boring 800-page book is by two Japanese mathematicians (whom I'll not name) and consists of about 16 million decimal digits of the number Te. "I assure you, Morris, that in spite of the beauty of the appar ent randomness of the decimal digits of Te, I'll be sure that my text will include also some words." And then I proceeded putting together the magic combina tion of words and numbers, which became The Book of Prime Number Records. If you have seen it, only extreme curiosity could impel you to have this one in your hands. The New Book of Prime Number Records differs little from its predecessor in the general planning. But it contains new sections and updated records.

Rather than focus on the technical details which can obscure the beauty of sieve theory, the authors focus on examples and applications, developing the theory in parallel.

Bridges the gap between theoretical and computational aspects of prime numbers Exercise sections are a goldmine of interesting examples, pointers to the literature and potential research projects Authors are well-known and highly-regarded in the field

The number field sieve is an algorithm for finding the prime factors of large integers. It depends on algebraic number theory. Proposed by John Pollard in 1988, the method was used in 1990 to factor the ninth Fermat number, a 155-digit integer. The algorithm is most suited to numbers of a special form, but there is a promising variant that applies in general. This volume contains six research papers that describe the operation of the number field sieve, from both theoretical and practical perspectives. Pollard's original manuscript is included. In addition, there is an annotated bibliography of directly related literature.

The authors assemble a fascinating collection of topics from analytic number theory that provides an introduction to the subject with a very clear and unique focus on the anatomy of integers, that is, on the study of the multiplicative structure of the integers. Some of the most important topics presented are the global and local behavior of arithmetic functions, an extensive study of smooth numbers, the Hardy-Ramanujan and Landau theorems, characters and the Dirichlet theorem, the abc conjecture along with some of its applications, and sieve methods. The book concludes with a whole chapter on the index of composition of an integer. One of this book's best features is the collection of problems at the end of each chapter that have been chosen carefully to reinforce the material. The authors include solutions to the even-numbered problems, making this volume very appropriate for readers who want to test their understanding of the theory presented in the book.

While taking a class on infinity at Stanford in the late 1980s, Ravi Kapoor discovers that he is confronting the same mathematical and philosophical dilemmas that his mathematician grandfather had faced many decades earlier--and that had landed him in jail. Charged under an obscure blasphemy law in a small New Jersey town in 1919, Vijay Sahni is challenged by a skeptical judge to defend his belief that the certainty of mathematics can be extended to all human knowledge--including religion. Together, the two men discover the power--and the fallibility--of what has long been considered the pinnacle of human certainty, Euclidean geometry. As grandfather and grandson struggle with the question of whether there can ever be absolute certainty in mathematics or life, they are forced to reconsider their fundamental beliefs and choices. Their stories hinge on their explorations of parallel developments in the study of geometry and infinity--and the mathematics throughout is as rigorous and fascinating as the narrative and characters are compelling and complex. Moving and enlightening, A Certain Ambiguity is a story about what it means to face the extent--and the limits--of human knowledge.

This book provides a motivated introduction to sieve theory. Rather than focus on technical details which obscure the beauty of the theory, the authors focus on examples and applications, developing the theory in parallel. Suitable for a senior level undergraduate course or an introductory graduate course in analytic number theory.