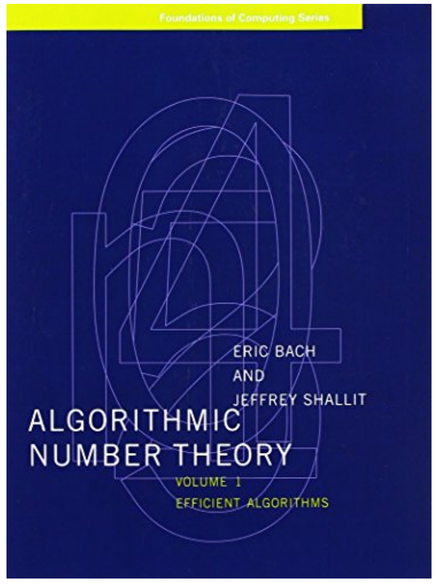

[Book] Algorithmic Number Theory: Efficient Algorithms (Foundations Of Computing)

As recognized, adventure as with ease as experience virtually lesson, amusement, as skillfully as settlement can be gotten by just checking out a books **Algorithmic Number Theory: Efficient Algorithms (Foundations of Computing)** along with it is not directly done, you could acknowledge even more almost this life, nearly the world.

We have enough money you this proper as competently as easy pretentiousness to get those all. We meet the expense of Algorithmic Number Theory: Efficient Algorithms (Foundations of Computing) and numerous books collections from fictions to scientific research in any way. along with them is this Algorithmic Number Theory: Efficient Algorithms (Foundations of Computing) that can be your partner.

Algorithmic Number Theory: Efficient algorithms-Eric Bach 1996 Volume 1.

Algorithmic Number Theory-Eric Bach 1996-08-26 Algorithmic Number Theory provides a thorough introduction to the design and analysis of algorithms for problems from the theory of numbers. Although not an elementary textbook, it includes over 300 exercises with suggested solutions. Every theorem not proved in the text or left as an exercise has a reference in the notes section that appears at the end of each chapter. The bibliography contains over 1,750 citations to the literature. Finally, it successfully blends computational theory with practice by covering some of the practical aspects of algorithm implementations.The subject of algorithmic number theory represents the marriage of number theory with the theory of computational complexity. It may be briefly defined as finding integer solutions to equations, or proving their non-existence, making efficient use of resources such as time and space. Implicit in this definition is the question of how to efficiently represent the objects in question on a computer. The problems of algorithmic number theory are important both for their intrinsic mathematical interest and their application to random number generation, codes for reliable and secure information transmission, computer algebra, and other areas.Publisher's Note: Volume 2 was not written. Volume 1 is, therefore, a stand-alone publication.

Algorithmic Number Theory-Claus Fieker 2003-08-02 This book constitutes the refereed proceedings of the 5th International Algorithmic Number Theory Symposium, ANTS-V, held in Sydney, Australia, in July 2002. The 34 revised full papers presented together with 5 invited papers have gone through a thorough round of reviewing, selection and revision. The papers are organized in topical sections on number theory, arithmetic geometry, elliptic curves and CM, point counting, cryptography, function fields, discrete logarithms and factoring, Groebner bases, and complexity.

Mathematics and Computation-Avi Wigderson 2019-10-29 An introduction to computational complexity theory, its connections and interactions with mathematics, and its central role in the natural and social sciences, technology, and philosophy Mathematics and Computation provides a broad, conceptual overview of computational complexity theory—the mathematical study of efficient computation. With important practical applications to computer science and industry, computational complexity theory has evolved into a highly interdisciplinary field, with strong links to most mathematical areas and to a growing number of scientific endeavors. Avi Wigderson takes a sweeping survey of complexity theory, emphasizing the field’s insights and challenges. He explains the ideas and motivations leading to key models, notions, and results. In particular, he looks at algorithms and complexity, computations and proofs, randomness and interaction, quantum and arithmetic computation, and cryptography and learning, all as parts of a cohesive whole with numerous cross-influences. Wigderson illustrates the immense breadth of the field, its beauty and richness, and its diverse and growing interactions with other areas of mathematics. He ends with a comprehensive look at the theory of computation, its methodology and aspirations, and the unique and fundamental ways in which it has shaped and will further shape science, technology, and society. For further reading, an extensive bibliography is provided for all topics covered. Mathematics and Computation is useful for undergraduate and graduate students in mathematics, computer science, and related fields, as well as researchers and teachers in these fields. Many parts require little background, and serve as an invitation to newcomers seeking an introduction to the theory of computation. Comprehensive coverage of computational complexity theory, and beyond High-level, intuitive exposition, which brings conceptual clarity to this central and dynamic scientific discipline Historical accounts of the evolution and motivations of central concepts and models A broad view of the theory of computation's influence on science, technology, and society Extensive bibliography

Algorithmic Number Theory- 2004

Algorithmic Number Theory-Wieb Bosma 2000-06-21 This book constitutes the refereed proceedings of the 4th International Algorithmic Number Theory Symposium, ANTS-IV, held in Leiden, The Netherlands, in July 2000. The book presents 36 contributed papers which have gone through a thorough round of reviewing, selection and revision. Also included are 4 invited survey papers. Among the topics addressed are gcd algorithms, primality, factoring, sieve methods, cryptography, linear algebra, lattices, algebraic number fields, class groups and fields, elliptic curves, polynomials, function fields, and power sums.

A Course in Computational Algebraic Number Theory-Henri Cohen 2013-04-17 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.

Number Theory for Computing-Song Y. Yan 2013-11-11 This book provides a good introduction to the classical elementary number theory and the modern algorithmic number theory, and their applications in computing and information technology, including computer systems design, cryptography and network security. In this second edition proofs of many theorems have been provided, further additions and corrections were made.

A Computational Introduction to Number Theory and Algebra-Victor Shoup 2005-04-28 This introductory book emphasises algorithms and applications, such as cryptography and error correcting codes.

Algorithms in a Nutshell-George T. Heineman 2008-10-14 Creating robust software requires the use of efficient algorithms, but programmers seldom think about them until a problem occurs. Algorithms in a Nutshell describes a large number of existing algorithms for solving a variety of problems, and helps you select and implement the right algorithm for your needs -- with just enough math to let you understand and analyze algorithm performance. With its focus on application, rather than theory, this book provides efficient code solutions in several programming languages that you can easily adapt to a specific project. Each major algorithm is presented in the style of a design pattern that includes information to help you understand why and when the algorithm is appropriate. With this book, you will: Solve a particular coding problem or improve on the performance of an existing solution Quickly locate algorithms that relate to the problems you want to solve, and determine why a particular algorithm is the right one to use Get algorithmic solutions in C, C++, Java, and Ruby with implementation tips Learn the expected performance of an algorithm, and the conditions it needs to perform at its best Discover the impact that similar design decisions have on different algorithms Learn advanced data structures to improve the efficiency of algorithms With Algorithms in a Nutshell, you'll learn how to improve the performance of key algorithms essential for the success of your software applications.

Algorithmic Algebraic Number Theory-M. Pohst 1997-09-25 Classic book, addressed to all lovers of number theory.

The LLL Algorithm-Phong Q. Nguyen 2009-12-02 The first book to offer a comprehensive view of the LLL algorithm, this text surveys computational aspects of Euclidean lattices and their main applications. It includes many detailed motivations, explanations and examples.

Algorithmic Cryptanalysis-Antoine Joux 2009-06-15 Illustrating the power of algorithms, Algorithmic Cryptanalysis describes algorithmic methods with cryptographically relevant examples. Focusing on both private- and public-key cryptographic algorithms, it presents each algorithm either as a textual description, in pseudo-code, or in a C code program. Divided into three parts, the book begins with a short introduction to cryptography and a background chapter on elementary number theory and algebra. It then moves on to algorithms, with each chapter in this section dedicated to a single topic and often illustrated with simple cryptographic applications. The final part addresses more sophisticated cryptographic applications, including LFSR-based stream ciphers and index calculus methods. Accounting for the impact of current computer architectures, this book explores the algorithmic and implementation aspects of cryptanalysis methods. It can serve as a handbook of algorithmic methods for cryptographers as well as a textbook for undergraduate and graduate courses on cryptanalysis and cryptography.

From Mathematics to Generic Programming-Alexander A. Stepanov 2014-11-13 In this substantive yet accessible book, pioneering software designer Alexander Stepanov and his colleague Daniel Rose illuminate the principles of generic programming and the mathematical concept of abstraction on which it is based, helping you write code that is both simpler and more powerful. If you’re a reasonably proficient programmer who can think logically, you have all the background you’ll need. Stepanov and Rose introduce the relevant abstract algebra and number theory with exceptional clarity. They carefully explain the problems mathematicians first needed to solve, and then show how these mathematical solutions translate to generic programming and the creation of more effective and elegant code. To demonstrate the crucial role these mathematical principles play in many modern applications, the authors show how to use these results and generalized algorithms to implement a real-world public-key cryptosystem. As you read this book, you’ll master the thought processes necessary for effective programming and learn how to generalize narrowly conceived algorithms to widen their usefulness without losing efficiency. You’ll also gain deep insight into the value of mathematics to programming—insight that will prove invaluable no matter what programming languages and paradigms you use. You will learn about How to generalize a four thousand-year-old algorithm, demonstrating indispensable lessons about clarity and efficiency Ancient paradoxes, beautiful theorems, and the productive tension between continuous and discrete A simple algorithm for finding greatest common divisor (GCD) and modern abstractions that build on it Powerful mathematical approaches to abstraction How abstract algebra provides the idea at the heart of generic programming Axioms, proofs, theories, and models: using mathematical techniques to organize knowledge about your algorithms and data structures Surprising subtleties of simple programming tasks and what you can learn from them How practical implementations can exploit theoretical knowledge

Twenty Lectures on Algorithmic Game Theory-Tim Roughgarden 2016-09-01 Computer science and economics have engaged in a lively interaction over the past fifteen years, resulting in the new field of algorithmic game theory. Many problems that are central to modern computer science, ranging from resource allocation in large networks to online advertising, involve interactions between multiple self-interested parties. Economics and game theory offer a host of useful models and definitions to reason about such problems. The flow of ideas also travels in the other direction, and concepts from computer science are increasingly important in economics. This book grew out of the author's Stanford University course on algorithmic game theory, and aims to give students and other newcomers a quick and accessible introduction to many of the most important concepts in the field. The book also includes case studies on online advertising, wireless spectrum auctions, kidney exchange, and network management.

Computational Complexity-Sanjeev Arora 2009-04-20 New and classical results in computational complexity, including interactive proofs, PCP, derandomization, and quantum computation. Ideal for graduate students.

Algorithmic Algebra-Bhubaneswar Mishra 1993-09-29 Algorithmic Algebra studies some of the main algorithmic tools of computer algebra, covering such topics as Gröbner bases, characteristic sets, resultants and semialgebraic sets. The main purpose of the book is to acquaint advanced undergraduate and graduate students in computer science, engineering and mathematics with the algorithmic ideas in computer algebra so that they could do research in computational algebra or understand the algorithms underlying many popular symbolic computational systems: Mathematica, Maple or Axiom, for instance. Also, researchers in robotics, solid modeling, computational geometry and automated theorem proving community may find it useful as symbolic algebraic techniques have begun to play an important role in these areas. The book, while being self-contained, is written at an advanced level and deals with the subject at an appropriate depth. The book is accessible to computer science students with no previous algebraic training. Some mathematical readers, on the other hand, may find it interesting to see how algorithmic constructions have been used to provide fresh proofs for some classical theorems. The book also contains a large number of exercises with solutions to selected exercises, thus making it ideal as a textbook or for self-study.

Algorithmic Problem Solving-Roland Backhouse 2011-10-24 An entertaining and captivating way to learn the fundamentals of using algorithms to solve problems The algorithmic approach to solving problems in computer technology is an essential tool. With this unique book, algorithm guru Roland Backhouse shares his four decades of experience to teach the fundamental principles of using algorithms to solve problems. Using fun and well-known puzzles to gradually introduce different aspects of algorithms in mathematics and computing. Backhouse presents you with a readable, entertaining, and energetic book that will motivate and challenge you to open your mind to the algorithmic nature of problem solving. Provides a novel approach to the mathematics of problem solving focusing on the algorithmic nature of problem solving Uses popular and entertaining puzzles to teach you different aspects of using algorithms to solve mathematical and computing challenges Features a theory section that supports each of the puzzles presented throughout the book Assumes only an elementary understanding of mathematics Let Roland Backhouse and his four decades of experience show you how you can solve challenging problems with algorithms!

Algorithmic Graph Theory-Alan Gibbons 1985-06-27 An introduction to pure and applied graph theory with an emphasis on algorithms and their complexity.

Advances in Cryptology--ASIACRYPT.- 2003

Algorithmic Number Theory- 1996

A Course in Computational Number Theory-David Bressoud 2008-06-10 A Course in Computational Number Theory uses the computer as a tool for motivation and explanation. The book is designed for the reader to quickly access a computer and begin doing personal experiments with the patterns of the integers. It presents and explains many of the fastest algorithms for working with integers. Traditional topics are covered, but the text also explores factoring algorithms, primality testing, the RSA public-key cryptosystem, and unusual applications such as check digit schemes and a computation of the energy that holds a salt crystal together. Advanced topics include continued fractions, Pell's equation, and the Gaussian primes.

Advances in Artificial Intelligence-Martin C. Golumbic 2012-12-06 Research in artificial intelligence, natural language processing and knowledge-based systems has blossomed during the past decade. At national and international symposia as well as in research centers and universities all over the world, these subjects have been the focus of intense debate and study. This is equally true in Israel which has hosted several international forums on these topics. The articles in this book represent a selection of contributions presented at recent AI conferences held in Israel. A theoretical model for a system that learns from its own experience in playing board games is presented in Learning from Experience in Board Games by Ze'ev Ben-Porat and Martin Golumbic. The model enables such a system to enhance and improve its playing capabilities through the use of a learning mechanism which extracts knowledge from actual playing experience. The learning process requires no external guidance or assistance. This model was implemented and tested on a variant of "Chinese Checkers. " The paper shows the feasibility and validity of the proposed model and investigates the parameters that affect its performance traits. The experimental results give evidence of the validity of the model as a powerful learning mechanism. Original and general algorithms for knowledge extraction and pattern matching were designed and tested as part of the prototype computer system. Analysis of the performance characteristics of these algorithms indicates that they can handle large knowledge bases in an efficient manner.

Understanding Machine Learning-Shai Shalev-Shwartz 2014-05-19 Introduces machine learning and its algorithmic paradigms, explaining the principles behind automated learning approaches and the considerations underlying their usage.

Algorithmic Principles of Mathematical Programming-Ulrich Faigle 2002-08-31 Algorithmic Principles of Mathematical Programming investigates the mathematical structures and principles underlying the design of efficient algorithms for optimization problems. Recent advances in algorithmic theory have shown that the traditionally separate areas of discrete optimization, linear programming, and nonlinear optimization are closely linked. This book offers a comprehensive introduction to the whole subject and leads the reader to the frontiers of current research. The prerequisites to use the book are very elementary. All the tools from numerical linear algebra and calculus are fully reviewed and developed. Rather than attempting to be encyclopedic, the book illustrates the important basic techniques with typical problems. The focus is on efficient algorithms with respect to practical usefulness. Algorithmic complexity theory is presented with the goal of helping the reader understand the concepts without having to become a theoretical specialist. Further theory is outlined and supplemented with pointers to the relevant literature. The book is equally suited for self-study for a motivated beginner and for a comprehensive course on the principles of mathematical programming within an applied mathematics or computer science curriculum at advanced undergraduate or graduate level. The presentation of the material is such that smaller modules on discrete optimization, linear programming, and nonlinear optimization can easily be extracted separately and used for shorter specialized courses on these subjects.

Modern Computer Arithmetic-Richard P. Brent 2010-11-25 Modern Computer Arithmetic focuses on arbitrary-precision algorithms for efficiently performing arithmetic operations such as addition, multiplication and division, and their connections to topics such as modular arithmetic, greatest common divisors, the Fast Fourier Transform (FFT), and the computation of elementary and special functions. Brent and Zimmermann present algorithms that are ready to implement in your favourite language, while keeping a high-level description and avoiding too low-level or machine-dependent details. The book is intended for anyone interested in the design and implementation of efficient high-precision algorithms for computer arithmetic, and more generally efficient multiple-precision numerical algorithms. It may also be used in a graduate course in mathematics or computer science, for which exercises are included. These vary considerably in difficulty, from easy to small research projects, and expand on topics discussed in the text. Solutions to selected exercises are available from the authors.

The Higher Arithmetic-H. Davenport 2008-10-23 The theory of numbers is generally considered to be the 'purest' branch of pure mathematics and demands exactness of thought and exposition from its devotees. It is also one of the most highly active and engaging areas of mathematics. Now into its eighth edition The Higher Arithmetic introduces the concepts and theorems of number theory in a way that does not require the reader to have an in-depth knowledge of the theory of numbers but also touches upon matters of deep mathematical significance. Since earlier editions, additional material written by J. H. Davenport has been added, on topics such as Wiles' proof of Fermat's Last Theorem, computers and number theory, and primality testing. Written to be accessible to the general reader, with only high school mathematics as prerequisite, this classic book is also ideal for undergraduate courses on number theory, and covers all the necessary material clearly and succinctly.

Complexity Theory-Ingo Wegener 2005-04-11 Reflects recent developments in its emphasis on randomized and approximation algorithms and communication models All topics are considered from an algorithmic point of view stressing the implications for algorithm design

Algorithms and Complexity-Herbert S. Wilf 2020-09-30 This book is an introductory textbook on the design and analysis of algorithms. The author uses a careful selection of a few topics to illustrate the tools for algorithm analysis. Recursive algorithms are illustrated by Quicksort, FFT, fast matrix multiplications, and others. Algorithms associated with the network flow problem are fundamental in many areas of graph connectivity, matching theory, etc. Algorithms in number theory are discussed with some applications to public key encryption. This second edition will differ from the present edition mainly in that solutions to most of the exercises will be included.

Annales Universitatis Scientiarum Budapestinensis de Rolando Eötvös Nominatae-Eötvös Loránd Tudományegyetem 2005

Semialgebraic Proofs and Efficient Algorithm Design-Noah Fleming 2019-12-10 The book provides the advanced reader with a deep insight into the exciting line of research, namely, proof that a solution exists has enabled an algorithm to find that solution itself with applications in many areas of computer science. It will inspire readers in deploying the techniques in their own further research.

Computing Roots in Finite Fields and Groups, with a Jaunt Through Sums of Digits-Scott Charles Lindhurst 1997

Numerical Algorithms-Justin Solomon 2015-06-24 Numerical Algorithms: Methods for Computer Vision, Machine Learning, and Graphics presents a new approach to numerical analysis for modern computer scientists. Using examples from a broad base of computational tasks, including data processing, computational photography, and animation, the textbook introduces numerical modeling and algorithmic desig

Mathematical Reviews- 2006

Smarandache Notions Journal- 2004

Dynamic Logic-David Harel 2000-09-29 This book provides the first comprehensive introduction to Dynamic Logic. Among the many approaches to formal reasoning about programs, Dynamic Logic enjoys the singular advantage of being strongly related to classical logic. Its variants constitute natural generalizations and extensions of classical formalisms. For example, Propositional Dynamic Logic (PDL) can be described as a blend of three complementary classical ingredients: propositional calculus, modal logic, and the algebra of regular events. In First-Order Dynamic Logic (DL), the propositional calculus is replaced by classical first-order predicate calculus. Dynamic Logic is a system of remarkable unity that is theoretically rich as well as of practical value. It can be used for formalizing correctness specifications and proving rigorously that those specifications are met by a particular program. Other uses include determining the equivalence of programs, comparing the expressive power of various programming constructs, and synthesizing programs from specifications. This book provides the first comprehensive introduction to Dynamic Logic. It is divided into three parts. The first part reviews the appropriate fundamental concepts of logic and computability theory and can stand alone as an introduction to these topics. The second part discusses PDL and its variants, and the third part discusses DL and its variants. Examples are provided throughout, and exercises and a short historical section are included at the end of each chapter.

Choice- 1996

Combinatorial Optimization-Christos H. Papadimitriou 2013-04-26 This graduate-level text considers the Soviet ellipsoid algorithm for linear programming; efficient algorithms for network flow, matching, spanning trees, and matroids; the theory of NP-complete problems; local search heuristics for NP-complete problems, more. 1982 edition.

Digital Signal Processing Algorithms-Hari Krishna 1998-03-25 Digital Signal Processing Algorithms describes computational number theory and its applications to deriving fast algorithms for digital signal processing. It demonstrates the importance of computational number theory in the design of digital signal processing algorithms and clearly describes the nature and structure of the algorithms themselves. The book has two primary focuses: first, it establishes the properties of discrete-time sequence indices and their corresponding fast algorithms; and second, it investigates the properties of the discrete-time sequences and the corresponding fast algorithms for processing these sequences. Digital Signal Processing Algorithms examines three of the most common computational tasks that occur in digital signal processing; namely, cyclic convolution, acyclic convolution, and discrete Fourier transformation. The application of number theory to deriving fast and efficient algorithms for these three and related computationally intensive tasks is clearly discussed and illustrated with examples. Its comprehensive coverage of digital signal processing, computer arithmetic, and coding theory makes Digital Signal Processing Algorithms an excellent reference for practicing engineers. The authors' intent to demystify the abstract nature of number theory and the related algebra is evident throughout the text, providing clear and precise coverage of the quickly evolving field of digital signal processing.

Algorithm Design: Pearson New International Edition-Jon Kleinberg 2013-08-29 August 6, 2009 Author, Jon Kleinberg, was recently cited in the New York Times for his statistical analysis research in the Internet age. Algorithm Design introduces algorithms by looking at the real-world problems that motivate them. The book teaches students a range of design and analysis techniques for problems that arise in computing applications. The text encourages an understanding of the algorithm design process and an appreciation of the role of algorithms in the broader field of computer science.