Prime Numbers A Computational Perspective

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

Requiring no more than a basic knowledge of abstract algebra, this text presents the mathematics of number fields in a straightforward, pedestrian manner. It therefore avoids local methods and presents proofs in a way that highlights the important parts of the arguments. Readers are assumed to be able to fill in the details, which in many places are left as exercises.

A comprehensive guide to mathematics with over 200 entries divided thematically.

This text originated as a lecture delivered November 20, 1984, at Queen's University, in the undergraduate colloquium series established to honour Professors A. J. Coleman and H. W. Ellis and to acknowledge their long-lasting interest in the quality of teaching undergraduate students. In another colloquium lecture, my colleague Morris Orzech, who had consulted the latest edition of the Guinness Book oj Records, reminded me very gently that the most "innumerate" people of the world are of a certain tribe 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 digits of the number 11. "I assure you Morris, that in spite of the beauty of the apparent randomness of the decimal digits of 11, I'll be sure that my text will also include some words." Acknowledgment. The manuscript of this book was prepared on the word processor by Linda Nuttall. I wish to express my appreciation for the great care, speed, and competence of her work. Paulo Ribenboim CONTENTS Preface vii Guiding the Reader xiii Index of Notations xv Introduction Chapter 1. How Many Prime Numbers Are There? 3 I. Euclid's Proof 3 II.

Computational Number Theory and Modern Cryptography

A Modern Approach

Real-Time C++

Prime Numbers

The Mathematical Gazette

Proceedings of the International Conference organized by the Stefan Banach International Mathematical Center Warsaw, Poland, September 11-15, 2000

The origins of the Asiacrypt series of conferences can be traced back to 1990, when the ?rst Auscrypt conference was held, although the name Asiacrypt was ?rst used for the 1991 conference in Japan. Starting with Asiacrypt 2000, the conference is now one of three annual conferences organized by the Inter- tional Association for Cryptologic Research (IACR). The continuing success of Asiacrypt is in no small part due to the e?c the Asiacrypt Steering C- mittee (ASC) and the strong support of the IACR Board of Directors. There were 153 papers submitted to Asiacrypt 2001 and 33 of these were accepted for inclusion in these proceedings. Th authors of every paper, whether accepted or not, made a valued contribution to the success of the conference. Sending out rejection noti?cations to so many hard working authors is one of the most unpleasant tasks o Program Chair. The review process lasted some 10 weeks and consisted of an initial refe- eing phase followed by an extensive discussion period. My heartfelt thanks go to all members of the Program Committee who extreme amounts of time to give their expert analysis and opinions on the submissions. All papers were reviewed by at least three committee members; in many cases, particularly for those papers submitted by comm members, additional reviews were obt- ned. Specialist reviews were provided by an army of external reviewers without whom our decisions would have been much more di?cult.

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 comp 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, randon 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 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 w 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 a 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

The fundamental mathematical tools needed to understand machine learning include linear algebra, analytic geometry, matrix decompositions, vector calculus, optimization, probability and statistics. These topics are traditionally taught in disparate courses, making it hard for data science or computer science students, or professionals, to efficiently learn the mathematics. This self-contained textbook bridges the gap between mathematical and machine learning texts, introducing the mathematical concepts with a minimum of prerequisites. It uses these concepts to derive four central machine learning methods: linear regression, principal component analysis, Gaussian mixture models and support vector machines. For students and others with a mathematical background, these derivations provide a starting point to machine learning texts. For those lea the mathematics for the first time, the methods help build intuition and practical experience with applying mathematical concepts. Every chapter includes worked examples and exercises to test understanding. Program tutorials are offered on the book's web site.

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 diffi 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 so 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 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 cyclo 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 i 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 exer

and 400 references.
Bernhard Riemann and the Greatest Unsolved Problem in Mathematics

Prime Numbers and Computer Methods for Factorization
A Historical and Technical Perspective
General Concepts and Techniques
Quantum Computing Since Democritus

The only book to provide a unified view of the interplay between computational number theory and cryptography Computational number theory and modern cryptography are two of the most important and fundamental research fields in information security. In this book, Song Y. Yang combines knowledge of these two critical fields, providing a unified view of the relationships between computational number theory and cryptography. The author takes an innovative approach, presenting mathematical ideas first, thereupon treating cryptography as an immediate application of the mathematical concepts. The book also presents topics from number theory, which are relevant for applications in public-key cryptography, as well as modern topics, such as coding and lattice based cryptography for post-quantum cryptography. The author further covers the current research and applications for common cryptographic algorithms, describing the mathematical problems behind these applications in a manner accessible to computer scientists and engineers. Makes mathematical problems accessible to computer scientists and engineers by showing their immediate application Presents topics from number theory relevant for public-key cryptography applications Covers modern topics such as coding and lattice based cryptography for post-quantum cryptography Starts with the basics, then goes into applications and areas of active research Geared at a global audience; classroom tested in North America, Europe, and Asia Incudes exercises in every chapter Instructor resources available on the book's Companion Website Computational Number Theory and Modern Cryptography is ideal for graduate and advanced undergraduate students in computer science, communications engineering, cryptography and mathematics. Computer scientists, practicing cryptographers, and other professionals involved in various security schemes will also find this book to be a helpful reference.
Originally published in 1934, this volume presents the theory of the distribution of the prime numbers in the series of natural numbers. Despite being long out of print, it remains unsurpassed as an introduction to the field.
Algorithms and Theory of Computation Handbook, Second Edition: General Concepts and Techniques provides an up-to-date compendium of fundamental computer science topics and techniques. It also illustrates how the topics and techniques come together to deliver efficient solutions to important practical problems. Along with updating and revising many of the existing chapters, this second edition contains four new chapters that cover external memory and parameterized algorithms as well as computational number theory and algorithmic coding theory. This best-selling handbook continues to help computer professionals and engineers find significant information on various algorithmic topics. The expert contributors clearly define the terminology, present basic results and techniques, and offer a number of current references to the in-depth literature. They also provide a glimpse of the major research issues concerning the relevant topics.
The subject of mathematics is not something distant, strange, and abstract that you can only learn about—and often dislike—in school. It is in everyday situations, such as housekeeping, communications, traffic, and weather reports. Taking you on a trip into the world of mathematics, Do I Count? Stories from Mathematics describes in a clear and captivating way the people behind the numbers and the places where mathematics is made. Written by top scientist and engaging storyteller Günter M. Ziegler and translated by Thomas von Foerster, the book presents mathematics and mathematicians in a manner that you have not previously encountered. It guides you on a scenic tour through the field, pointing out which beds were useful in constructing which theorems and which notebooks list the prizes for solving particular problems. Forgoing esoteric areas, the text relates mathematics to celebrities, history, travel, politics, science and technology, weather, clever puzzles, and the future. Can bees count? Is 13 bad luck? Are there equations for everything? What's the real practical value of the Pythagorean Theorem? Are there Sudoku puzzles with fewer than 17 entries and just one solution? Where and how do mathematicians work? Who invented proofs and why do we need them? Why is there no Nobel Prize for mathematics? What kind of life did Paul Erd?s lead? Find out the answers to these and other questions in this entertaining book of stories. You'll see that everyone counts, but no computation is needed.
7th International Conference on the Theory and Application of Cryptology and Information Security Gold Coast, Australia, December 9–13, 2001. Proceedings
Complexity and Real Computation
Algorithms and Theory of Computation Handbook, Second Edition, Volume 1
Prime Obsession
A Computational Perspective
Efficient Object-Oriented and Template Microcontroller Programming

From the original hard cover edition: In the modern age of almost universal computer usage, practically every individual in a technologically developed society has routine access to the most up-to-date cryptographic technology that exists, the so-called RSA public-key cryptosystem. A major component of this system is the factorization of large numbers into their primes. Thus an ancient number-theory concept now plays a crucial role in communication among millions of people who may have little or no knowledge of even elementary mathematics. Hans Riesel's highly successful first edition of this book has now been enlarged and updated with the goal of satisfying the needs of researchers, students, practitioners of cryptography, and non-scientific readers with a mathematical inclination. It includes important advances in computational prime number theory and in factorization as well as re-computed and enlarged tables, accompanied by new tables reflecting current research by both the author and his coworkers and by independent researchers. The book treats four fundamental problems: the number of primes below a given limit, the approximate number of primes, the recognition of primes and the factorization of large numbers. The author provides explicit algorithms and computer programs, and has attempted to discuss as many of the classically important results as possible, as well as the most recent discoveries. The programs include are written in PASCAL to allow readers to translate the programs into the language of their own computers. The independent structure of each chapter of the book makes it highly readable for a wide variety of mathematicians, students of applied number theory, and others interested in both study and research in number theory and cryptography.

Research Paper from the year 2012 in the subject Computer Science - Applied, Northcentral University, language: English, abstract: Paper discusses Goldbach's Conjecture that all even integers can be represented as the sum of two prime numbers and presents an algorithm to verify the conjecture which is only limited by the size of the primes that can be generated.

The Proceedings contain twenty selected, refereed contributions arising from the International Conference on Public-Key Cryptography and Computational Number Theory held in Warsaw, Poland, on September 11-15, 2000. The conference, attended by eightyfive mathematicians from eleven countries, was organized by the Stefan Banach International Mathematical Center. This volume contains articles from leading experts in the world on cryptography and computational number theory, providing an account of the state of research in a wide variety of topics related to the conference theme. It is dedicated to the memory of the Polish mathematicians Marian Rejewski (1905-1980), Jerzy Róøycki (1909-1942) and Henryk Zygalski (1907-1978), who deciphered the military version of the famous Enigma in December 1932 - January 1933. A noteworthy feature of the volume is a foreword written by Andrew Odlyzko on the progress in cryptography from Enigma time until now.

This introductory book emphasises algorithms and applications, such as cryptography and error correcting codes.

Advances in Cryptology — ASIACRYPT 2001

A Computational Introduction to Number Theory and Algebra

Stories from Mathematics

A Theory Revolutionizing Technology and Science

Bulletin of the Belgian Mathematical Society, Simon Stevin

Bulletin (new Series) of the American Mathematical Society

Takes students and researchers on a tour through some of the deepest ideas of maths, computer science and physics.

This book is about the theory and practice of integer factorisation presented in a historic perspective. It describes about twenty algorithms for factoring and a dozen other number theory algorithms that support the factoring algorithms. Most algorithms are described both in words and in pseudocode to satisfy both number theorists and computer scientists. Each of the ten chapters begins with a concise summary of its contents. The book starts with a general explanation of why factoring integers is important. The next two chapters present number theory results that are relevant to factoring. Further on there is a chapter discussing, in particular, mechanical and electronic devices for factoring, as well as factoring using quantum physics and DNA molecules. Another chapter applies factoring to breaking certain cryptographic algorithms. Yet another chapter is devoted to practical vs. theoretical aspects of factoring. The book contains more than 100 examples illustrating various algorithms and theorems. It also contains more than 100 interesting exercises to test the reader's understanding. Hints or answers are given for about a third of the exercises. The book concludes with a dozen suggestions of possible new methods for factoring integers. This book is written for readers who want to learn more about the best methods of factoring integers, many reasons for factoring, and some history of this fascinating subject. It can be read by anyone who has taken a first course in number theory.

Algorithms and Theory of Computation Handbook, Second Edition in a two volume set, provides an up-to-date compendium of fundamental computer science topics and techniques. It also illustrates how the topics and techniques come together to deliver efficient solutions to important practical problems. New to the Second Edition: Along with updating and revising many of the existing chapters, this second edition contains more than 20 new chapters. This edition now covers external memory, parameterized, self-stabilizing, and pricing algorithms as well as the theories of algorithmic coding, privacy and anonymity, databases, computational games, and communication networks. It also discusses computational topology, computational number theory, natural language processing, and grid computing and explores applications in intensity-modulated radiation therapy, voting, DNA research, systems biology, and financial derivatives. This best-selling handbook continues to help computer professionals and engineers find significant information on various algorithmic topics. The expert contributors clearly define the terminology, present basic results and techniques, and offer a number of current references to the in-depth literature. They also provide a glimpse of the major research issues concerning the

relevant topics
In this book the author treats four fundamental and apparently simple problems. They are: the number of primes below a given limit, the ap proximate number of primes, the recognition of prime numbers and the factorization of large numbers. A chapter on the details of the distribution of the primes is included as well as a short description of a recent applica tion of prime numbers, the so-called RSA public-key cryptosystem. The author is also giving explicit algorithms and computer programs. Whilst not claiming completeness, the author has tried to give all important results known, including the latest discoveries. The use of computers has in this area promoted a development which has enormously enlarged the wealth of results known and that has made many older works and tables obsolete. As is often the case in number theory, the problems posed are easy to understand but the solutions are theoretically advanced. Since this text is aimed at the mathematically inclined layman, as well as at the more advanced student, not all of the proofs of the results given in this book are shown. Bibliographical references in these cases serve those readers who wish to probe deeper. References to recent original works are also given for those who wish to pursue some topic further. Since number theory is seldom taught in basic mathematics courses, the author has appended six sections containing all the algebra and number theory required for the main body of the book.
Advances in Cryptology--ASIACRYPT.
The Book of Prime Number Records
Public-Key Cryptography and Computational Number Theory
The Distribution of Prime Numbers
Gaither's Dictionary of Scientific Quotations
The Computer as Crucible
This is a book about prime numbers, congruences, secret messages, and elliptic curves that you can read cover to cover. It grew out of undergr- uate courses that the author taught at Harvard, UC San Diego, and the University of Washington. The systematic study of number theory was initiated around 300B. C. when Euclid proved that there are in?nitely many prime numbers, and also cleverly deduced the fundamental theorem of arithmetic, which asserts that every positive integer factors uniquely as a product of primes. Over a thousand years later (around 972A. D.) Arab mathematicians formulated the congruent number problem that asks for a way to decide whether or not a given positive integer n is the area of a right triangle, all three of whose sides are rational numbers. Then another thousand years later (in 1976), Di?e and Hellman introduced the ?rst ever public-key cryptosystem, which enabled two people to communicate secretely over a public communications channel with no predetermined secret; this invention and the ones that followed it revolutionized the world of digital communication. In the 1980s and 1990s, elliptic curves revolutionized number theory, providing striking new insights into the congruent number problem, primality testing, publ- key cryptography, attacks on public-key systems, and playing a central role in Andrew Wiles' resolution of Fermat's Last Theorem.
Prime NumbersA Computational PerspectiveSpringer Science & Business Media
With this book, Christopher Kormanyos delivers a highly practical guide to programming real-time embedded microcontroller systems in C++. It is divided into three parts plus several appendices. Part I provides a foundation for real-time C++ by covering language technologies, including object-oriented methods, template programming and optimization. Next, part II presents detailed descriptions of a variety of C++ components that are widely used in microcontroller programming. It details some of C++'s most powerful language elements, such as class types, templates and the STL, to develop components for microcontroller register access, low-level drivers, custom memory management, embedded containers, multitasking, etc. Finally, part III describes mathematical methods and generic utilities that can be employed to solve recurring problems in real-time C++. The appendices include a brief C++ language tutorial, information on the real-time C++ development environment and instructions for building GNU GCC cross-compilers and a microcontroller circuit. For this third edition, the most recent specification of C++17 in ISO/IEC 14882:2017 is used throughout the text. Several sections on new C++17 functionality have been added, and various others reworked to reflect changes in the standard. Also several new sample projects are introduced and existing ones extended, and various user suggestions have been incorporated. To facilitate portability, no libraries other than those specified in the language standard itself are used. Efficiency is always in focus and numerous examples are backed up with real-time performance measurements and size analyses that quantify the true costs of the code down to the very last byte and microsecond. The target audience of this book mainly consists of students and professionals interested in real-time C++. Readers should be familiar with C or another programming

language and will benefit most if they have had some previous experience with microcontroller electronics and the performance and size issues prevalent in embedded systems programming.

*The classical theory of computation has its origins in the work of Goedel, Turing, Church, and Kleene and has been an extraordinarily successful framework for theoretical computer science. The thesis of this book, however, is that it provides an inadequate foundation for modern scientific computation where most of the algorithms are real number algorithms. The goal of this book is to develop a formal theory of computation which integrates major themes of the classical theory and which is more directly applicable to problems in mathematics, numerical analysis, and scientific computing. Along the way, the authors consider such fundamental problems as: * Is the Mandelbrot set decidable? * For simple quadratic maps, is the Julia set a halting set? * What is the real complexity of Newton's method? * Is there an algorithm for deciding the knapsack problem in a ploynomial number of steps? * Is the Hilbert Nullstellensatz intractable? * Is the problem of locating a real zero of a degree four polynomial intractable? * Is linear programming tractable over the reals? The book is divided into three parts: The first part provides an extensive introduction and then proves the fundamental NP-completeness theorems of Cook-Karp and their extensions to more general number fields as the real and complex numbers. The later parts of the book develop a formal theory of computation which integrates major themes of the classical theory and which is more directly applicable to problems in mathematics, numerical analysis, and scientific computing.*

Mathematics and Computation

Quantum Computation and Quantum Information

A Collection of Approximately 27,000 Quotations Pertaining to Archaeology, Architecture, Astronomy, Biology, Botany, Chemistry, Cosmology, Darwinism, Engineering, Geology, Mathematics, Medicine, Nature, Nursing, Paleontology, Philosophy, Physics, Probability, Science, Statistics, Technology, Theory, Universe, and Zoology

Computing

Verifying Goldbach's Conjecture

The Joy of Factoring

First-ever comprehensive introduction to the major new subject of quantum computing and quantum information.

In the modern age of almost universal computer usage, practically every individual in a technologically developed society has routine access to the most up-to-date cryptographic technology that exists, the so-called RSA public-key cryptosystem. A major component of this system is the factorization of large numbers into their primes. Thus an ancient number-theory concept now plays a crucial role in communication among millions of people who may have little or no knowledge of even elementary mathematics. The independent structure of each chapter of the book makes it highly readable for a wide variety of mathematicians, students of applied number theory, and others interested in both study and research in number theory and cryptography.

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.

Keith Devlin and Jonathan Borwein, two well-known mathematicians with expertise in different mathematical specialties but with a common interest in experimentation in mathematics, have joined forces to create this introduction to experimental mathematics. They cover a variety of topics and examples to give the reader a good sense of the current sta

Not Always Buried Deep

Elementary Number Theory: Primes, Congruences, and Secrets

An Introduction to Experimental Mathematics

Do I Count?

An Experimental Introduction to Number Theory

Computational Complexity

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.

This book presents material suitable for an undergraduate course in elementary number theory from a computational perspective. It seeks to not only introduce students to the standard topics in elementary number theory, such as prime factorization and modular arithmetic, but also to develop their ability to formulate and test precise conjectures from experimental data. Each topic is motivated by a question to be answered, followed by some experimental data, and, finally, the statement and proof of a theorem. There are numerous opportunities throughout the chapters and exercises for the students to engage in (guided) open-ended exploration. At the end of a course using this book, the students will understand how mathematics is developed from asking questions to gathering data to formulating and proving theorems. The mathematical prerequisites for this book are few. Early chapters contain topics such as integer divisibility, modular arithmetic, and applications to cryptography, while later chapters contain more specialized topics, such as Diophantine approximation, number theory of dynamical systems, and number theory with polynomials. Students of all levels will be drawn in by the patterns and relationships of number theory uncovered through data driven exploration.

This marvellous and highly original book fills a significant gap in the extensive literature on classical modular forms. This is not just yet another introductory text to this theory, though it could certainly be used as such in conjunction with more traditional treatments. Its novelty lies in its computational emphasis throughout: Stein not only defines what modular forms are, but shows in illuminating detail how one can compute everything about them in practice. This is illustrated throughout the book with examples from his own (entirely free) software package SAGE, which really bring the subject to life while not detracting in any way from its theoretical beauty. The author is the leading expert in computations with modular forms, and what he says on this subject is all tried and tested and based on his extensive experience. As well as being an invaluable companion to those learning the theory in a more traditional way, this book will be a great help to those who wish to use modular forms in applications, such as in the explicit solution of Diophantine equations. There is also a useful Appendix by Gunnells on extensions to more general modular forms, which has enough in it to inspire many PhD theses for years to come. While the book's main readership will be graduate students in number theory, it will also be accessible to advanced undergraduates and useful to both specialists and non-specialists in number theory. --John E. Cremona, University of Nottingham William Stein is an associate professor of mathematics at the University of Washington at Seattle. He earned a PhD in mathematics from UC Berkeley and has held positions at Harvard University and UC San Diego. His current research interests lie in modular forms, elliptic curves, and computational mathematics.

New and classical results in computational complexity, including interactive proofs, PCP, derandomization, and quantum computation. Ideal for graduate students.

The Prime Numbers and Their Distribution

Modular Forms, a Computational Approach

A Second Course in Elementary Number Theory

Bulletin of the American Mathematical Society

A Computational Approach

Mathematics for Machine Learning

This unprecedented collection of 27,000 quotations is the most comprehensive and carefully researched of its kind, covering all fields of science and mathematics. With this vast compendium you can readily conceptualize and embrace the written images of scientists, laymen, politicians, novelists, playwrights, and poets about humankind's scientific achievements. Approximately 9000 high-quality entries have been added to this new edition to provide a rich selection of quotations for the student, the educator, and the scientist who would like to introduce a presentation with a relevant quotation that provides perspective and historical background on his subject. Gaither's Dictionary of Scientific Quotations, Second Edition, provides the finest reference source of science quotations for all audiences. The new edition adds greater depth to the number of quotations in the various thematic arrangements and also provides new thematic categories.

Exploring a vast array of topics related to computation, Computing: A Historical and Technical Perspective covers the historical and technical foundation of ancient and modern-day computing. The book starts with the earliest references to counting by humans, introduces various number systems, and discusses mathematics in early civilizations. It guides readers all the way through the latest advances in computer science, such as the design and analysis of computer algorithms. Through historical accounts, brief technical explanations, and examples, the book answers a host of questions, including: Why do humans count differently from the way current electronic computers do? Why are there 24 hours in a day, 60 minutes in an hour, etc.? Who invented numbers, when were they invented, and why are there different kinds? How do secret writings and cryptography date back to ancient civilizations? Innumerable individuals from many cultures have contributed their talents and creativity to formulate what has become our mathematical and computing heritage. By bringing together the historical and technical aspects of computing, this book enables readers to gain a deep appreciation of the long evolutionary processes of the field developed over thousands of years. Suitable as a supplement in undergraduate courses, it provides a self-contained historical reference source for anyone interested in this important and evolving field.

In August 1859 Bernhard Riemann, a little-known 32-year old mathematician, presented a paper to the Berlin Academy titled: "On the Number of Prime Numbers Less Than a Given Quantity." In the middle of that paper, Riemann made an incidental remark â € " a guess, a hypothesis. What he tossed out to the assembled mathematicians that day has proven to be almost cruelly compelling to countless scholars in the ensuing years. Today, after 150 years of careful research and exhaustive study, the question remains. Is the hypothesis true or false? Riemann's basic inquiry, the primary topic of his paper, concerned a straightforward but nevertheless important matter of arithmetic â € " defining a precise formula to track and identify the occurrence of prime numbers. But it is that incidental remark â € " the Riemann Hypothesis â € " that is the truly astonishing legacy of his 1859 paper. Because Riemann was able to see beyond the pattern of the primes to discern traces of something mysterious and mathematically elegant shrouded in the shadows â € " subtle variations in the distribution of those prime numbers. Brilliant for its clarity, astounding for its potential consequences, the Hypothesis took on enormous importance in mathematics. Indeed, the successful solution to this puzzle would herald a revolution in prime number theory. Proving or disproving it became the greatest challenge of the age. It has become clear that the Riemann Hypothesis, whose resolution seems to hang tantalizingly just beyond our grasp, holds the key to a variety of scientific and mathematical investigations. The making and breaking of modern codes, which depend on the properties of the prime numbers, have roots in the Hypothesis. In a series of extraordinary developments during the 1970s, it emerged that even the physics of the atomic nucleus is connected in ways not yet fully understood to this strange conundrum. Hunting down the solution to the Riemann Hypothesis has become an obsession for many â € " the veritable "great white whale" of mathematical research. Yet despite determined efforts by generations of mathematicians, the Riemann Hypothesis defies resolution. Alternating passages of extraordinarily lucid

mathematical exposition with chapters of elegantly composed biography and history, Prime Obsession is a fascinating and fluent account of an epic mathematical mystery that continues to challenge and excite the world. Posited a century and a half ago, the Riemann Hypothesis is an intellectual feast for the cognoscenti and the curious alike. Not just a story of numbers and calculations, Prime Obsession is the engrossing tale of a relentless hunt for an elusive proof â € " and those who have been consumed by it.

Number Fields

Modern Computer Arithmetic

The Princeton Companion to Mathematics

Algorithms and Theory of Computation Handbook - 2 Volume Set