Discrete Algebraic Methods Arithmetic Cryptograph

Codes, Cryptology and Curves with Computer Algebra
Computational Number Theory
A Course in Mathematical Cryptography
Topics in Infinite Group Theory
Discrete Mathematics
Mathematical Foundations of Public Key Cryptography
Chaos-based Cryptography
Discrete Mathematics
Cryptology
Discrete Mathematics
Discrete Algebraic Methods
Algebraic and Discrete Mathematical Methods for Modern Biology
Applied Algebra, Algebraic Algorithms and Error-Correcting Codes
An Introduction to Mathematical Cryptography
Introduction to Cryptography with Mathematical Foundations and Computer Implementations
Abstract Algebra
Graphs for Pattern Recognition
Algebra and Number Theory
Concrete Mathematics
Complexity and Randomness in Group Theory
Algebraic Aspects of Cryptography
Advances in Cryptology - ASIACRYPT 2000
Number Theoretic Methods in Cryptography
Elliptic Curves
Introductory Discrete Mathematics
Advanced Number Theory with Applications
Mathematics of Public Key Cryptography
Farey Sequences
Combinatorics on Words
Arithmetic, Geometry, Cryptography and Coding Theory
Algorithms and Architectures for Cryptography and Source Coding in Non-Volatile Flash Memories
A Course in Number Theory and Cryptography
Computational Number Theory and Modern Cryptography
Applied Algebra
Algebraic Curves in Cryptography
Discrete Mathematics With Cryptographic Applications
Discrete Mathematics
Applied Algebra, Algebraic Algorithms and Error-Correcting Codes
Finitely Presented Groups
International Conference of Computational Methods in Sciences and Engineering (ICCMSE 2004)

MARISA MATA

Codes, Cryptology and Curves with Computer Algebra Springer Science & Business Media
This book gives an advanced overview of several topics in infinite group theory. It can also be considered as a rigorous introduction to combinatorial and geometric group theory. The philosophy of the book is to describe the interaction between these two important parts of infinite group theory. In this line of thought, several theorems are proved multiple times with different methods either purely combinatorial or purely geometric while others are shown by a combination of arguments from both perspectives. The first part of the book deals with Nielsen methods and introduces the reader to results and examples that are helpful to understand the following parts. The second part focuses on covering spaces and fundamental groups, including covering space proofs of group theoretic results. The third part deals with the theory of hyperbolic groups. The subjects are illustrated and described by prominent examples and an outlook on solved and unsolved problems. New edition now includes the topics on universal free groups, quasiconvex subgroups and hyperbolic groups, and also Stallings foldings and subgroups of free groups. New results on groups of F-types are added.
Computational Number Theory CRC Press
This concise, undergraduate-level text focuses on combinatorics, graph theory with applications to some standard network optimization problems, and algorithms. More than 200 exercises, many with complete solutions. 1991 edition.
A Course in Mathematical Cryptography CRC Press
Using mathematical tools from number theory and finite fields, Applied Algebra: Codes, Ciphers, and Discrete Algorithms, Second Edition presents practical methods for solving problems in data security and data integrity. It is designed for an applied algebra course for students who have had prior classes in abstract or linear algebra. While the con
Topics in Infinite Group Theory Walter de Gruyter GmbH & Co KG
The reach of algebraic curves in cryptography goes far beyond elliptic curve or public key cryptography yet these other application areas have not been systematically covered in the literature. Addressing this gap, Algebraic Curves in Cryptography explores the rich uses of algebraic curves in a range of cryptographic applications, such as secret sh
Discrete Mathematics Springer Nature
Like its bestselling predecessor, Elliptic Curves: Number Theory and Cryptography, Second Edition develops the theory of elliptic curves to provide a basis for both number theoretic and cryptographic applications. With additional exercises, this edition offers more comprehensive coverage of the fundamental theory, techniques, and application
Mathematical Foundations of Public Key Cryptography Walter de Gruyter GmbH & Co KG
This self-contained introduction to modern cryptography emphasizes the mathematics behind the theory of public key cryptosystems and digital signature schemes. The book focuses on these key topics while developing the mathematical tools needed for the construction and security analysis of diverse cryptosystems. Only basic linear algebra is required of the reader; techniques from algebra, number theory, and probability are introduced and developed as required. This text provides an ideal introduction for mathematics and computer science students to the mathematical foundations of modern cryptography. The book includes an extensive bibliography and index; supplementary materials are available online. The book covers a variety of topics that are considered central to mathematical cryptography. Key topics include: classical cryptographic constructions, such as Diffie–Hellmann key exchange, discrete logarithm-based cryptosystems, the RSA cryptosystem, and digital signatures; fundamental mathematical tools for cryptography, including primality testing, factorization algorithms, probability theory, information theory, and collision algorithms; an in-depth treatment of important cryptographic innovations, such as elliptic curves, elliptic curve and pairing-based cryptography, lattices, lattice-based cryptography, and the NTRU cryptosystem. The second edition of An Introduction to Mathematical Cryptography includes a significant revision of the material on digital signatures, including an earlier introduction to RSA, Elgamal, and DSA signatures, and new material on lattice-based signatures and rejection sampling. Many sections have been rewritten or expanded for clarity, especially in the chapters on information theory, elliptic curves, and lattices, and the chapter of additional topics has been expanded to include sections on digital cash and homomorphic encryption. Numerous new exercises have been included.
Chaos-based Cryptography John Wiley & Sons
This is a substantially revised and updated introduction to arithmetic topics, both ancient and modern, that have been at the centre of interest in applications of number theory, particularly in cryptography. As such, no background in algebra or number theory is assumed, and the book begins with a discussion of the basic number theory that is needed. The approach taken is algorithmic, emphasising estimates of the efficiency of the techniques that arise from the theory, and one special feature is the inclusion of recent applications of the theory of elliptic curves. Extensive exercises and careful answers are an integral part all of the chapters.
Discrete Mathematics Walter de Gruyter GmbH & Co KG
This monograph deals with mathematical constructions that are foundational in such an important area of data mining as pattern recognition. By using combinatorial and graph theoretic techniques, a closer look is taken at infeasible systems of linear inequalities, whose generalized solutions act as building blocks of geometric decision rules for pattern recognition. Infeasible systems of linear inequalities prove to be a key object in pattern recognition problems described in geometric terms thanks to the committee method. Such infeasible systems of inequalities represent an important special subclass of infeasible systems of constraints with a monotonicity property – systems whose multi-indices of feasible subsystems form abstract simplicial complexes (independence systems), which are fundamental objects of combinatorial topology. The methods of data mining and machine learning discussed in this monograph form the foundation of technologies like big data and deep learning, which play a growing role in many areas of human-technology interaction and help to find solutions, better solutions and excellent solutions. Contents: Preface Pattern recognition, infeasible systems of linear inequalities, and graphs Infeasible monotone systems of constraints Complexes, (hyper)graphs, and inequality systems Polytopes, positive bases, and inequality systems Monotone Boolean functions, complexes, graphs, and inequality systems Inequality systems, committees, (hyper)graphs, and alternative covers Bibliography List of notation Index
Cryptology Walter de Gruyter GmbH & Co KG
This book shows new directions in group theory motivated by computer science. It reflects the transition from geometric group theory to group theory of the 21st century that has strong connections to computer science. Now that geometric group theory is drifting further and further away from group theory to geometry, it is natural to look for new tools and new directions in group theory which are present.
Discrete Mathematics Springer Science & Business Media
This book covers discrete mathematics both as it has been established after its emergence since the middle of the last century and as its elementary applications to cryptography. It can be used by any individual studying discrete mathematics, finite mathematics, and similar subjects. Any necessary prerequisites are explained and illustrated in the book. As a background of cryptography, the textbook gives an introduction into number theory, coding theory, information theory, that obviously have discrete nature. FEATURES: Designed in a “self-teaching” format, the book includes about 600 problems (with and without solutions) and numerous examples of cryptography Covers

cryptography topics such as CRT, affine ciphers, hashing functions, substitution ciphers, unbreakable ciphers, Discrete Logarithm Problem (DLP), and more.

Discrete Algebraic Methods Cambridge University Press

This book introduces the mathematics that supports advanced computer programming and the analysis of algorithms. The primary aim of its well-known authors is to provide a solid and relevant base of mathematical skills - the skills needed to solve complex problems, to evaluate horrendous sums, and to discover subtle patterns in data. It is an indispensable text and reference not only for computer scientists - the authors themselves rely heavily on it! - but for serious users of mathematics in virtually every discipline. Concrete Mathematics is a blending of CONtinuous and disCRETE mathematics. "More concretely," the authors explain, "it is the controlled manipulation of mathematical formulas, using a collection of techniques for solving problems." The subject matter is primarily an expansion of the Mathematical Preliminaries section in Knuth's classic Art of Computer Programming, but the style of presentation is more leisurely, and individual topics are covered more deeply. Several new topics have been added, and the most significant ideas have been traced to their historical roots. The book includes more than 500 exercises, divided into six categories. Complete answers are provided for all exercises, except research problems, making the book particularly valuable for self-study. Major topics include: Sums Recurrences Integer functions Elementary number theory Binomial coefficients Generating functions Discrete probability Asymptotic methods This second edition includes important new material about mechanical summation. In response to the widespread use of the first edition as a reference book, the bibliography and index have also been expanded, and additional nontrivial improvements can be found on almost every page. Readers will appreciate the informal style of Concrete Mathematics. Particularly enjoyable are the marginal graffiti contributed by students who have taken courses based on this material. The authors want to convey not only the importance of the techniques presented, but some of the fun in learning and using them.

Algebraic and Discrete Mathematical Methods for Modern Biology Springer Science & Business Media

The book introduces new techniques which imply rigorous lower bounds on the complexity of some number theoretic and cryptographic problems. These methods and techniques are based on bounds of character sums and numbers of solutions of some polynomial equations over finite fields and residue rings. It also contains a number of open problems and proposals for further research. We obtain several lower bounds, exponential in terms of logp, on the de grees and orders of • polynomials; • algebraic functions; • Boolean functions; • linear recurring sequences; coinciding with values of the discrete logarithm modulo a prime p at suf ficiently many points (the number of points can be as small as pI/He). These functions are considered over the residue ring modulo p and over the residue ring modulo an arbitrary divisor d of p - 1. The case of d = 2 is of special interest since it corresponds to the representation of the right most bit of the discrete logarithm and defines whether the argument is a quadratic residue. We also obtain non-trivial upper bounds on the de gree, sensitivity and Fourier coefficients of Boolean functions on bits of x deciding whether x is a quadratic residue. These results are used to obtain lower bounds on the parallel arithmetic and Boolean complexity of computing the discrete logarithm. For example, we prove that any unbounded fan-in Boolean circuit. of sublogarithmic depth computing the discrete logarithm modulo p must be of superpolynomial size.

Applied Algebra, Algebraic Algorithms and Error-Correcting Codes Springer

The idea behind this book is to provide the mathematical foundations for assessing modern developments in the Information Age. It deepens and complements the basic concepts, but it also considers instructive and more advanced topics. The treatise starts with a general chapter on algebraic structures; this part provides all the necessary knowledge for the rest of the book. The next chapter gives a concise overview of cryptography. Chapter 3 on number theoretic algorithms is important for developping cryptosystems, Chapter 4 presents the deterministic primality test of Agrawal, Kayal, and Saxena. The account to elliptic curves again focuses on cryptographic applications and algorithms. With combinatorics on words and automata theory, the reader is introduced to two areas of theoretical computer science where semigroups play a fundamental role.The last chapter is devoted to combinatorial group theory and its connections to automata. Contents: Algebraic structures Cryptography Number theoretic algorithms Polynomial time primality test Elliptic curves Combinatorics on words Automata Discrete infinite groups

An Introduction to Mathematical Cryptography Academic Press

In Mathematical Foundations of Public Key Cryptography, the authors integrate the results of more than 20 years of research and teaching experience to help students bridge the gap between math theory and crypto practice. The book provides a theoretical structure of fundamental number theory and algebra knowledge supporting public-key cryptography.R

Introduction to Cryptography with Mathematical Foundations and Computer Implementations Walter de Gruyter GmbH & Co KG

The International Conference of Computational Methods in Sciences and Engineering (ICCMSE) is unique in its kind. It regroups original contributions from all fields of the traditional Sciences, Mathematics, Physics, Chemistry, Biology, Medicine and all branches of Engineering. The aim of the conference is to bring together computational scientists from several disciplines in order to share methods and ideas. More than 370 extended abstracts have been submitted for consideration for presentation in ICCMSE 2004. From these, 289 extended abstracts have been selected after international peer review by at least two independent reviewers.

Abstract Algebra Mercury Learning and Information

Cryptology: Classical and Modern, Second Edition proficiently introduces readers to the fascinating field of cryptology. The book covers classical methods including substitution, transposition, Playfair, ADFGVX, Alberti, Vigene re, and Hill ciphers. It also includes coverage of the Enigma machine, Turing bombe, and Navajo code. Additionally, the book presents modern methods like RSA, ElGamal, and stream ciphers, as well as the Diffie-Hellman key exchange and Advanced Encryption Standard. When possible, the book details methods for breaking both classical and modern methods. The new edition expands upon the material from the first edition which was oriented for students in non-technical fields. At the same time, the second edition supplements this material with new content that serves students in more technical fields as well. Thus, the second edition can be fully utilized by both technical and non-technical students at all levels of study. The authors include a wealth of material for a one-semester cryptology course, and research exercises that can be used for supplemental projects. Hints and answers to selected exercises are found at the end of the book.

Graphs for Pattern Recognition Courier Corporation

From the reviews: "This is a textbook in cryptography with emphasis on algebraic methods. It is supported by many exercises (with answers) making it appropriate for a course in mathematics or computer science. [...] Overall, this is an excellent expository text, and will be very useful to both the student and researcher." Mathematical Reviews

Algebra and Number Theory Springer Science & Business Media

Developed from the author's popular graduate-level course, Computational Number Theory presents a complete treatment of number-theoretic algorithms. Avoiding advanced algebra, this self-contained text is designed for advanced undergraduate and beginning graduate students in engineering. It is also suitable for researchers new to the field and pract

Concrete Mathematics CRC Press

This book constitutes the refereed proceedings of the 15th International Symposium on Applied Algebra, Algebraic Algorithms and Error-Correcting Codes, AAECC-15, held in Toulouse, France, in May 2003. The 25 revised full papers presented together with 2 invited papers were carefully reviewed and selected from 40 submissions. Among the subjects addressed are block codes; algebra and codes: rings, fields, and AG codes; cryptography; sequences; decoding algorithms; and algebra: constructions in algebra, Galois groups, differential algebra, and polynomials.

Complexity and Randomness in Group Theory CRC Press

This advanced graduate textbook gives an authoritative and insightful description of the major ideas and techniques of public key cryptography.