Equations Over Finite Fields An Elementary Approach

The theory of elliptic curves involves a blend of algebra, geometry, analysis, and number theory. This book stresses this interplay as it develops the basic theory, providing an opportunity for readers to appreciate the unity of modern mathematics. The book's accessibility, the informal writing style, and a wealth of exercises make it an ideal introduction for those interested in learning about Diophantine equations and arithmetic geometry.

Lacunary Polynomials Over Finite Fields focuses on reducible lacunary polynomials over finite fields, as well as stem polynomials, differential equations, and gaussian sums. The monograph first tackles preliminaries and formulation of Problems I, II, and III, including some basic concepts and notations, invariants of polynomials, stem polynomials, fully reducible polynomials, and polynomials with a restricted range. The text then takes a look at Problem I and reduction of Problem II to Problem III. Topics include reduction of the marginal case of Problem II to that of Problem III, proposition on power series, proposition on polynomials, and preliminary remarks on polynomial and differential equations. The publication ponders on Problem III and applications. Topics include homogeneous elementary symmetric systems of equations in finite fields; divisibility maximum properties of the gaussian sums and related questions; common representative systems of a finite abelian group with respect to given subgroups; and difference quotient of functions in finite fields. The monograph also reviews certain families of linear mappings in finite fields, appendix on the degenerate solutions of Problem II, a lemma on the greatest common divisor of polynomials with common gap, and two group-theoretical propositions. The text is a dependable reference for mathematicians and researchers interested in the study of reducible lacunary polynomials over finite fields.

Crypto '90 marked the tenth anniversary of the Crypto conferences held at the University of California at Santa Barbara. The conference was held from August 11 to August 15, 1990 and was sponsored by the International Association for Cryptologic Research, in cooperation with the IEEE Computer Society Technical Committee on Security and Privacy and the Department of Computer Science of the University of California at Santa Barbara. 227 participants from twenty countries around the world. Crypto '90 attracted Roughly 35% of attendees were from academia, 45% from industry and 20% from government. The program was intended to provide a balance between the purely theoretical and the purely practical aspects of cryptography to meet the needs and diversified interests of these various groups. The overall organization of the conference was superbly handled by the general chairperson Sherry McMahan. All of the outstanding features of Crypto, which we have come to expect over the years, were again present and, in addition to all of this, she did a magnificent job in the preparation of the book of abstracts. This is a crucial part of the program and we owe her a great deal of thanks.

Solving Non-sparse Systems of Linear Equations Over Finite Fields on the CM-5

Equations Over Finite Fields

Algorithmic Number Theory: Efficient algorithms

Rational Points on Elliptic Curves

This book constitutes the refereed proceedings of the Third International Workshop on the Arithmetic of Finite Fields, WAIFI 2010, held in Istanbul, Turkey, in June 2010. The 15 revised full papers presented were carefully reviewed and selected from 33 submissions. The papers are organized in topical sections on efficient finite field arithmetic, pseudo-random numbers and sequences, Boolean functions, functions, Equations and modular multiplication, finite field arithmetic for pairing based cryptography, and finite field, cryptography and coding.

This book is devoted entirely to the theory of finite fields.

ABSTRACT: Let F q to the t be the finite field with q to the t elements and let F q to the t star be its multiplicative group. We study the diagonal equation a times x to the (q minus 1) plus b times y to the (q minus 1) equals c, where a, b and c are elements of F q to the t star. This equation can be written as x to the (q minus 1) plus alpha times y to the (q minus 1) equals beta, where alpha and beta are elements of F q to the t star. Let N sub t (alpha, beta) denote the number of solutions (x, y) in F q to the t star cross F q to the t star of the equation x to the (q minus 1) plus alpha times y to the (q minus 1) equals beta and I(r;a, b) be the number of monic irreducible polynomials f with coefficients in F q of degree r with f(0) equals a and f(1) equals b. We show that N sub t (alpha, beta) can be expressed in terms of I(r;a, b), where r divides t and a, b are elements of F q star are related to alpha and beta. A recursive formula for I(r;a, b) will be given and we illustrate this by computing I(r;a, b) for r greater than or equal to 2 but less than or equal to 4. We also show that N sub 3 (alpha, beta) can be expressed in terms of the number of monic irreducible cubic polynomials over F q with prescribed trace and norm. Connsequently, N sub 3 (alpha, beta) can be expressed in terms of the number of rational points on a certain elliptic curve. We give a proof that given any a, b elements of F q star and integer r greater than or equal to 3, there always exists a monic irreducible polynomial f with coefficients in F q of degree r such that f(0) equals a and f(1) equals b. We also use the result on N sub 2 (alpha, beta) to construct a new family of planar functions.

Counting Polynomial Matrices over Finite Fields

Including an Introduction to Equations Over Finite Fields

Third International Workshop, WAIFI 2010, Istanbul, Turkey, June 27-30, 2010, Proceedings

Applications of Curves Over Finite Fields

Certain Diagonal Equations Over Finite Fields

V.1. A.N. v.2. O.Z. Apendices and indexes.

This book provides an accessible and self-contained introduction to the theory of algebraic curves over a finite field, a subject that has been of fundamental importance to mathematics for many years and that has essential applications in areas such as finite geometry, number theory, error-correcting codes, and cryptology. Unlike other books, this one emphasizes the algebraic geometry rather than the function field approach to algebraic curves. The authors begin by developing the general theory of curves over any field, highlighting peculiarities occurring for positive characteristic and requiring of the reader only basic knowledge of algebra and geometry. The special properties that a curve over a finite field can have are then discussed. The geometrical theory of linear series is used to find estimates for the number of rational points on a curve, following the theory of St ö hr and Voloch. The approach of Hasse and Weil via zeta functions is explained, and then attention turns to more advanced results: a state-of-the-art introduction to maximal curves over finite fields is provided; a comprehensive account is given of the automorphism group of a curve; and some applications to coding theory and finite geometry are described. The book includes many examples and exercises. It is an indispensable resource for researchers and the ideal textbook for graduate students.
This book is concerned with two areas of mathematics, at first sight disjoint, and with some of the analogies and interactions between them. These areas are the theory of linear differential equations in one complex variable with polynomial coefficients, and the theory of one parameter families of exponential sums over finite fields. After reviewing some results from representation theory, the book discusses results about differential equations and their differential galois groups (G) and one-parameter families of exponential sums and their geometric monodromy groups (G). The final part of the book is devoted to comparison theorems relating G and G of suitably "corresponding" situations, which provide a systematic explanation of the remarkable "coincidences" found "by hand" in the hypergeometric case.
Arithmetic of Finite Fields
Set Theory and Hierarchy Theory
Finite Fields
EQUATIONS IN FINITE FIELDS..
On Solving Univariate Polynomial Equations Over Finite Fields and Some Related Problems
The first part of this book presents an introduction to the theory of finite fields, with emphasis on those aspects that are relevant for applications. The second part is devoted to a discussion of the most important applications of finite fields especially information theory, algebraic coding theory and cryptology (including some very recent material that has never before appeared in book form). There is also a chapter on applications within mathematics, such as finite geometries. combinatorics. and pseudorandom sequences. Worked-out examples and list of exercises found throughout the book make it useful as a textbook.
Poised to become the leading reference in the field, the Handbook of Finite Fields is exclusively devoted to the theory and applications of finite fields. More than 80 international contributors compile state-of-the-art research in this definitive handbook. Edited by two renowned researchers, the book uses a uniform style and format throughout and
Equations over Finite FieldsAn Elementary ApproachSpringerSet Theory and Hierarchy TheoryA Memorial Tribute to Andrzej Mostowski : Bierotowice, Poland, 1975 : [proceedings]Equations Over Finite FieldsAn Elementary ApproachElements of Number TheoryIncluding an Introduction to Equations Over Finite FieldsEquations Over Finite FieldsEquations Over Finite Fields and Their SolutionsAdvances in Cryptology - CRYPTO '90ProceedingsSpringer
Solutions of Equations Over Finite Fields
Lectures on Finite Fields
Algebraic Curves over Finite Fields
Proceedings
Kumar's Algorithm for Solving Toeplitz Systems of Equations Over Finite Fields
Because of their applications in so many diverse areas, finite fields continue to play increasingly important roles in various branches of modern mathematics, including number theory, algebra, and algebraic geometry, as well as in computer science, information theory, statistics, and engineering. Computational and algorithmic aspects of finite field problems also continue to grow in importance. This volume contains the refereed proceedings of a conference entitled Finite Fields: Theory, Applications and Algorithms, held in August 1993 at the University of Nevada at Las Vegas. Among the topics treated are theoretical aspects of finite fields, coding theory, cryptology, combinatorial design theory, and algorithms related to finite fields. Also included is a list of open problems and conjectures. This volume is an excellent reference for applied and research mathematicians as well as specialists and graduate students in information theory, computer science, and electrical engineering.
Text for a one-semester course at the advanced undergraduate/beginning graduate level, or reference for algebraists and mathematicians interested in algebra, algebraic geometry, and number theory, examines counting or estimating numbers of solutions of equations in finite fields concentrating on top
This volume presents the results of the AMS-IMS-SIAM Joint Summer Research Conference held at the University of Washington (Seattle). The talks were devoted to various aspects of the theory of algebraic curves over finite fields and its numerous applications. The three basic themes are the following: Curves with many rational points. Several articles describe main approaches to the construction of such curves: the Drinfeld modules and fiber product methods, the moduli space approach, and the constructions using classical curves; Monodromy groups of characteristic p covers. A number of authors presented the results and conjectures related to the study of the monodromy groups of curves over finite fields. In particular, they study the monodromy groups from genus 0 covers, reductions of covers, and explicit computation of monodromy groups over finite fields; and, Zeta functions and trace formulas.To a large extent, papers devoted to this topic reflect the contributions of Professor Bernard Dwork and his students. This conference was the last attended by Professor Dwork before his death, and several papers inspired by his presence include commentaries about the applications of trace formulas and L-function. The volume also contains a detailed introduction paper by Professor Michael Fried, which helps the reader to navigate in the material presented in the book.
Algorithms for Solving Linear and Polynomial Systems of Equations Over Finite Fields with Applications to Cryptanalysis
Algebraic Curves Over a Finite Field
Encyclopedic Dictionary of Mathematics
Matrices with Certain Primeness Properties and Applications to Linear Systems and Coding Theory
A Removal Lemma for Systems of Linear Equations Over Finite Fields
The theory of finite fields encompasses algebra, combinatorics, and number theory and has furnished widespread applications in other areas of mathematics and computer science. This book is a collection of selected topics in the theory of finite fields and related areas. The topics include basic facts about finite fields, polynomials over finite fields, Gauss sums, algebraic number theory and cyclotomic fields, zeros of polynomials over finite fields, and classical groups over finite fields. The book is mostly self-contained, and the material

covered is accessible to readers with the knowledge of graduate algebra; the only exception is a section on function fields. Each chapter is supplied with a set of exercises. The book can be adopted as a text for a second year graduate course or used as a reference by researchers.

This book is dealing with three mathematical areas, namely polynomial matrices over finite fields, linear systems and coding theory. Primeness properties of polynomial matrices provide criteria for the reachability and observability of interconnected linear systems. Since time-discrete linear systems over finite fields and convolutional codes are basically the same objects, these results could be transferred to criteria for non-catastrophicity of convolutional codes. In particular, formulas for the number of pairwise coprime polynomials and for the number of mutually left coprime polynomial matrices are calculated. This leads to the probability that a parallel connected linear system is reachable and that a parallel connected convolutional code is non-catastrophic. Moreover, other networks of linear systems and convolutional codes are considered.

This title provides a self-contained introduction to the theory of algebraic curves over a finite field, whose origins can be traced back to the works of Gauss and Galois on algebraic equations in two variables with coefficients modulo a prime number.

1997 AMS-IMS-SIAM Joint Summer Research Conference on Applications of Curves Over Finite Fields, July 27-31, 1997, University of Washington, Seattle

Introduction to Finite Fields and Their Applications

Exponential Sums and Differential Equations

Note on Systems of Polynomial Equations Over Finite Fields

Systems of Diagonal Equations Over Finite Fields

In this tract, Professor Moreno develops the theory of algebraic curves over finite fields, their zeta and L-functions, and, for the first time, the theory of algebraic geometric Goppa codes on algebraic curves. Among the applications considered are: the problem of counting the number of solutions of equations over finite fields; Bombieri's proof of the Reimann hypothesis for function fields, with consequences for the estimation of exponential sums in one variable; Goppa's theory of error-correcting codes constructed from linear systems on algebraic curves; there is also a new proof of the TsfasmanSHVladutSHZink theorem. The prerequisites needed to follow this book are few, and it can be used for graduate courses for mathematics students. Electrical engineers who need to understand the modern developments in the theory of error-correcting codes will also benefit from studying this work.

Algebraic Cryptanalysis bridges the gap between a course in cryptography, and being able to read the cryptanalytic literature. This book is divided into three parts: Part One covers the process of turning a cipher into a system of equations; Part Two covers finite field linear algebra; Part Three covers the solution of Polynomial Systems of Equations, with a survey of the methods used in practice, including SAT-solvers and the methods of Nicolas Courtois. Topics include: Analytic Combinatorics, and its application to cryptanalysis The equicomplexity of linear algebra operations Graph coloring Factoring integers via the quadratic sieve, with its applications to the cryptanalysis of RSA Algebraic Cryptanalysis is designed for advanced-level students in computer science and mathematics as a secondary text or reference book for self-guided study. This book is suitable for researchers in Applied Abstract Algebra or Algebraic Geometry who wish to find more applied topics or practitioners working for security and communications companies.

Volume 1.

Lectures on equations over finite fields

Handbook of Finite Fields

Algebraic Cryptanalysis

Solutions to Systems of Equations Over Finite Fields

Equations over Finite Fields

Abstract: "Let F be a finite field of q elements and characteristic p (so q = p[superscript n] for some n [> or =] 1) and let [gamma] := [formula] be a system of polynomial equations with coefficients in F. In this paper we relate the structure of the F-algebra [formula] to the roots of [gamma] in F[superscript r]."

Algebraic Curves over a Finite Field

Elements of Number Theory

Theory, Applications, and Algorithms

Matric Equations and Canonical Forms Over Finite Fields

Equations Over Finite Fields and Their Solutions