Equations Over Finite Fields An Elementary Approach

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

Develops the theory of algebraic curves over finite fields, their zeta and L-functions and the theory of algebraic geometric Goppa codes.

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 Stöhr 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 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.

Volume 1.

This volume contains the proceedings of the 10th International Congress on Finite Fields and their Applications (Fq 10), held July 11-15, 2011, in Ghent, Belgium. Research on finite fields and their practical applications continues to flourish. This volume's topics, which include finite geometry, finite semifields, bent functions, polynomial theory, designs, and function fields, show the variety of research in this area and prove the tremendous importance of finite field theory.

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.

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 ApproachEquations over Finite FieldsAn Elementary ApproachEquations Over Finite FieldsElements of Number TheoryIncluding an Introduction to Equations Over Finite FieldsNote on Systems of Polynomial Equations Over Finite Fields

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

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.

This volume contains the proceedings of the Ninth International Conference on Finite

Fields and Applications, held in Ireland, July 13-17, 2009. It includes survey papers by all invited speakers as well as selected contributed papers. Finite fields continue to grow in mathematical importance due to applications in many diverse areas. This volume contains a variety of results advancing the theory of finite fields and connections with, as well as impact on, various directions in number theory, algebra, and algebraic geometry. Areas of application include algebric coding theory, cryptology, and combinatorial design theory.

This book constitutes the refereed proceedings of the 4th International Workshop on the Arithmetic of Finite Field, WAIFI 2012, held in Bochum, Germany, in July 2012. The 13 revised full papers and 4 invited talks presented were carefully reviewed and selected from 29 submissions. The papers are organized in topical sections on coding theory and code-based cryptography, Boolean functions, finite field arithmetic, equations and functions, and polynomial factorization and permutation polynomial.

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]."

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.

The book introduces new techniques that imply rigorous lower bounds on the com plexity of some number-theoretic and cryptographic problems. It also establishes certain attractive pseudorandom properties of various cryptographic primitives. These methods and techniques are based on bounds of character sums and num bers of solutions of some polynomial equations over finite fields and residue rings. Other number theoretic techniques such as sieve methods and lattice reduction algorithms are used as well. The book also contains a number of open problems and proposals for further research. The emphasis is on obtaining

unconditional rigorously proved statements. The bright side of this approach is that the results do not depend on any assumptions or conjectures. On the downside, the results are much weaker than those which are widely believed to be true. We obtain several lower bounds, exponential in terms of logp, on the degrees and orders of o polynomials; o algebraic functions; o Boolean functions; o linear recurrence sequences; coinciding with values of the discrete logarithm modulo a prime p at sufficiently many points (the number of points can be as small as pI/2+O:). 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 rightmost bit of the discrete logarithm and defines whether the argument is a quadratic residue.

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

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.

This book is mainly devoted to some computational and algorithmic problems in finite fields such as, for example, polynomial factorization, finding irreducible and primitive polynomials, the distribution of these primitive polynomials and of primitive points on elliptic curves, constructing bases of various types and new applications of finite fields to other areas of mathematics. For completeness we in clude two special chapters on some recent advances and applications of the theory of congruences (optimal coefficients, congruential pseudo-random number gener ators, modular arithmetic, etc.) and computational number theory (primality testing, factoring integers, computation in algebraic number theory, etc.). The problems considered here have many applications in Computer Science, Cod ing Theory, Cryptography, Numerical Methods, and so on. There are a few books devoted to more general questions, but the results contained in this book have not till now been collected under one cover. In the present work the author has attempted to point out new links among different areas of the theory of finite fields. It contains many very important results which previously could be found only in widely scattered and hardly available conference proceedings and journals. In particular, we extensively review results which originally appeared

only in Russian, and are not well known to mathematicians outside the former USSR.

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 volume contains the proceedings of the 11th International Conference on Finite Fields and their Applications (Fq11), held July 22-26, 2013, in Magdeburg, Germany. Finite Fields are fundamental structures in mathematics. They lead to interesting deep problems in number theory, play a major role in combinatorics and finite geometry, and have a vast amount of applications in computer science. Papers in this volume cover these aspects of finite fields as well as applications in coding theory and cryptography.