Algebraic Function Fields And Codes

NEVEAH JONATHAN

On Splitting Places of Degree One in Extensions of Algebraic Function Fields, Towers of Function Fields Meeting Asymptotic Bounds, and Basis Constructions for Algebraic-geometric Codes Springer Science & Business Media
Algebraic number theory is one of the most refined creations in mathematics. It has been developed by some of the leading mathematicians of this and previous centuries. The primary goal of this book is to present the essential elements of algebraic number theory, including the theory of normal extensions up through a glimpse of class field theory. Following the example set for us by Kronecker, Weber, Hilbert and Artin, algebraic functions are handled here on an equal footing with algebraic numbers. This is done on the one hand to demonstrate the analogy between number fields and function fields, which is especially clear in the case where the ground field is a finite field. On the other hand, in this way one obtains an introduction to the theory of 'higher congruences' as an important element of 'arithmetic geometry'. Early chapters discuss topics in elementary number theory, such as Minkowski's geometry of numbers, public-key cryptography and a short proof of the Prime Number Theorem, following Newman and Zagier. Next, some of the tools of algebraic number theory are introduced, such as ideals, discriminants and valuations. These results are then applied to obtain results about function fields, including a proof of the Riemann-Roch Theorem and, as an application of cyclotomic fields, a proof of the first case of Fermat's Last Theorem. There are a detailed exposition of the theory of Hecke L-series, following Tate, and explicit applications to number theory, such as the Generalized Riemann Hypothesis. Chapter 9 brings together the earlier material through the study of quadratic number fields. Finally, Chapter 10 gives an introduction to class field theory. The book attempts as much as possible to give simple proofs. It can be used by a beginner in algebraic number theory who wishes to see some of the true power and depth of the subject. The book is suitable for two one-semester courses, with the first four chapters serving to develop the basic material. Chapters 6 through 9 could be used on their own as a second semester course.
Riemann-Roch Spaces and Computation Springer Science & Business Media
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.
Field Arithmetic Springer Science & Business Media

The series is aimed specifically at publishing peer reviewed reviews and contributions presented at workshops and conferences. Each volume is associated with a particular conference, symposium or workshop. These events cover various topics within pure and applied mathematics and provide up-to-date coverage of new developments, methods and applications.
Algebraic Geometric Codes: Basic Notions American Mathematical Society
Thisseries is devoted to the publication of monographs, lecture resp. seminar notes, and other materials arising from programs of the OSU Mathemaical Research Institute. This includes proceedings of conferences or workshops held at the Institute, and other mathematical writings.
Advances in Algebraic Geometry Codes American Mathematical Soc.
This volume covers many topics, including number theory, Boolean functions, combinatorial geometry, and algorithms over finite fields. It contains many new, theoretical and applicable results, as well as surveys that were presented by the top specialists in these areas. New results include an answer to one of Serre''s questions, posted in a letter to Top; cryptographic applications of the discrete logarithm problem related to elliptic curves and hyperelliptic curves; construction of function field towers; construction of new classes of Boolean cryptographic functions; and algorithmic applications of algebraic geometry. Sample Chapter(s). Chapter 1: Fast addition on non-hyperelliptic genus 3 curves (424 KB). Contents: Symmetric Cryptography and Algebraic Curves (F Voloch); Galois Invariant Smoothness Basis (J-M Couveignes & R Lercier); Fuzzy Pairing-Based CL-PKC (M Kiviharju); On the Semiprimitivity of Cyclic Codes (Y Aubry & P Langevin); Decoding of Scroll Codes (G H Hitching & T Johnsen); An Optimal Unramified Tower of Function Fields (K Brander); On the Number of Resilient Boolean Functions (S Mesnager); On Quadratic Extensions of Cyclic Projective Planes (H F Law & P P W Wong); Partitions of Vector Spaces over Finite Fields (Y Zelenyuk); and other papers. Readership: Mathematicians, researchers in mathematics (academic and industry R&D).
Topics in Geometry, Coding Theory and Cryptography Walter de Gruyter
The inaugural research program of the Institute for Mathematical Sciences at the National University of Singapore took place from July to December 2001 and was devoted to coding theory and cryptology. As part of the program, tutorials for graduate students and junior researchers were given by world-renowned scholars. These tutorials covered fundamental aspects of coding theory and cryptology and were designed to prepare for original research in these areas. The present volume collects the expanded lecture notes of these tutorials. The topics range from mathematical areas such as computational number theory, exponential sums and algebraic function fields through coding-theory subjects such as extremal problems, quantum error-correcting codes and algebraic-geometry codes to cryptologic subjects such as stream ciphers, public-key infrastructures, key management, authentication schemes and distributed system security. Contents:Extremal Problems of Coding Theory (A Barg)Analysis and Design Issues for Synchronous Stream Ciphers (E Dawson & L Simpson)Quantum Error-Correcting Codes (K Feng)Public Key Infrastructures (D Gollmann)Computational Methods in Public Key Cryptology (A K Lenstra)Detecting and Revoking Compromised Keys (T Matsumoto)Algebraic Function Fields Over Finite Fields (H Niederreiter)Authentication Schemes (D Y Pei)Exponential Sums in Coding Theory, Cryptology and Algorithms (I E Shparlinski)Distributed Authorization: Principles and Practice (V Varadharajan)Introduction to Algebraic Geometry Codes (C P Xing) Readership: Graduate students and researchers in number theory, discrete mathematics, coding theory, cryptology and IT security. Keywords:Coding Theory;Cryptology;Number Theory;Algebraic-Geometry Codes;Public-Key Infrastructures;Error-Correcting Codes
Analytic Arithmetic of Algebraic Function Fields Walter de Gruyter
The fields of algebraic functions of one variable appear in several areas of mathematics: complex analysis, algebraic geometry, and number theory. This text adopts the latter perspective by applying an arithmetic-algebraic viewpoint to the study of function fields as part of the algebraic theory of numbers. The examination explains both the similarities and fundamental differences between function fields and number fields, including many exercises and examples to enhance understanding and motivate further study. The only prerequisites are a basic knowledge of field theory, complex analysis, and some commutative algebra.
Number Theory Springer Science & Business Media
This book is an introduction to the theory of algebraic numbers and algebraic functions of one variable. The basic development is the same for both using E Artin's legant approach, via valuations. Number Theory is pursued as far as the unit theorem and the finiteness of the class number. In function theory the aim is the Abel-Jacobi theorem describing the devisor class group, with occasional geometrical asides to help understanding. Assuming only an undergraduate course in algebra, plus a little acquaintance with topology and complex function theory, the book serves as an introduction to more technical works in algebraic number theory, function theory or algebraic geometry by an exposition of the central themes in the subject.
Analytic Arithmetic of Algebraic Function Fields Cambridge University Press
Develops the theory of algebraic curves over finite fields, their zeta and L-functions and the theory of algebraic geometric Goppa codes.
Codes from Certain Algebraic Function Fields with Many Rational Places Springer Science & Business Media
Presents an approach to algebraic geometry of curves that is treated as the theory of algebraic functions on the curve. This book discusses such topics as the theory of divisors on a curve, the Riemann-Roch theorem, p-adic completion, and extensions of the fields of functions (covering theory) and of the fields of constants.
Algebraic Geometry Codes: Advanced Chapters Springer
Advances in Algebraic Geometry Codes presents the most successful applications of algebraic geometry to the field of error-correcting codes, which are used in the industry when one sends information through a noisy channel. The noise in a channel is the corruption of a part of the information due to either interferences in the telecommunications or degradation of the information-storing support (for instance, compact disc). An error-correcting code thus adds extra information to the message to be transmitted with the aim of recovering the sent information. With contributions from renowned researchers, this pioneering book will be of value to mathematicians, computer scientists, and engineers in information theory.
Introductory Notes on Valuation Rings and Function Fields in One Variable World Scientific
The book focuses on the educational perspective of Riemann-Roch spaces and the computation of algebraic structures connected to the Riemann-Roch theorem, which is a useful tool in fields of complex analysis and algebraic geometry. On one hand, the theorem connects the Riemann surface with its topological genus, and on the other it allows us to compute the algebraic function field spaces. In the first part of this book, algebraic structures and some of their properties are presented. The second part shows efficient algorithms and examples connected to Riemann-Roch spaces. What is important, a variety of examples with codes of algorithms are given in the book, covering the majority of the cases.
Coding Theory and Cryptology Algebraic Function Fields and Codes
This book provides an exposition of function field arithmetic with emphasis on recent developments concerning Drinfeld modules, the arithmetic of special values of transcendental functions (such as zeta and gamma functions and their interpolations), diophantine approximation and related interesting open problems. While it covers many topics treated in 'Basic Structures of Function Field Arithmetic' by David Goss, it complements that book with the inclusion of recent developments as well as the treatment of new topics such as diophantine approximation, hypergeometric functions, modular forms, transcendence, automata and solitons. There is also new work on multizeta values and log-algebraicity. The author has included numerous worked-out examples. Many open problems, which can serve as good thesis problems, are discussed.
Vorstellung der Königlichen Frnzösischen Seemacht Cambridge University Press
Early in the development of number theory, it was noticed that the ring of integers has many properties in common with the ring of polynomials over a finite field. The first part of this book illustrates this relationship by presenting analogues of various theorems. The later chapters probe the analogy between global function fields and algebraic number fields. Topics include the ABC-conjecture, Brumer-Stark conjecture, and Drinfeld modules.
Cohomological Theory of Crystals Over Function Fields Princeton University Press
This book develops a new cohomological theory for schemes in positive characteristic p and it applies this theory to give a purely algebraic proof of a conjecture of Goss on the rationality of certain L-functions arising in the arithmetic of function fields. These L-functions are power series over a certain ring A, associated to any family of Drinfeld A-modules or, more generally, of A-motives on a variety of finite type over the finite field $\mathbb{F}_p$. By analogy to the Weil conjecture, Goss conjectured that these L-functions are in fact rational functions. In 1996 Taguchi and Wan gave a first proof of Goss's conjecture by analytic methods a la Dwork. The present text introduces A-crystals, which can be viewed as generalizations of families of A-motives, and studies their cohomology. While A-crystals are defined in terms of coherent sheaves together with a Frobenius map, in many ways they actually behave like constructible etale sheaves. A central result is a Lefschetz trace formula for L-functions of A-crystals, from which the rationality of these L-functions is immediate. Beyond its application to Goss's L-functions, the theory of A-crystals is closely related to the work of Emerton and Kisin on unit root F-crystals, and it is essential in an Eichler - Shimura type isomorphism for Drinfeld modular forms as constructed by the first author. The book is intended for researchers and advanced graduate students interested in the arithmetic of function fields and/or cohomology theories for varieties in positive characteristic. It assumes a good working knowledge in algebraic geometry as well as familiarity with homological algebra and derived categories, as provided by standard textbooks. Beyond that the presentation is largely self contained.
Topics in the Theory of Algebraic Function Fields American Mathematical Soc.
This textbook equips graduate students and advanced undergraduates with the necessary theoretical tools for applying algebraic geometry to information theory, and it covers primary applications in coding theory and cryptography. Harald Niederreiter and Chaoping Xing provide the first detailed discussion of the interplay between nonsingular projective curves and algebraic function fields over finite fields. This interplay is fundamental to research in the field today, yet until now no other textbook has featured complete proofs of it. Niederreiter and Xing cover classical applications like algebraic-geometry codes and elliptic-curve cryptosystems as well as material not treated by other books, including function-field codes, digital nets, code-based public-key cryptosystems, and frameproof codes. Combining a systematic development of theory with a broad selection of real-world applications, this is the most comprehensive yet accessible introduction to the field available. Introduces graduate students and advanced undergraduates to the foundations of algebraic geometry for applications to information theory Provides the first detailed discussion of the interplay between projective curves and algebraic function fields over finite fields Includes applications to coding theory and cryptography Covers the latest advances in algebraic-geometry codes Features applications to cryptography not treated in other books
Algebraic Function Fields and Codes Princeton University Press
Discussion of theory and applications of algebraic curves over finite fields with many rational points.
Basic Structures of Function Field Arithmetic European Mathematical Society
The book deals with the (elementary and introductory) theory of valuation rings. As explained in the introduction, this represents a useful and important viewpoint in algebraic geometry, especially concerning the theory of algebraic curves and their function fields. The correspondences of this with other viewpoints (e.g. of geometrical or topological nature) are often indicated, also to provide motivations and intuition for many results. Links with arithmetic are also often indicated. There are three appendices, concerning Hilbert’s Nullstellensatz (for which several proofs are provided), Puiseux series and Dedekind domains. There are also several exercises, often accompanied by hints, which sometimes develop further results not included in full for brevity reasons.
Algebraic Curves Over Finite Fields Springer Science & Business Media
These notes are based on lectures given in the semmar on "Coding Theory and Algebraic Geometry" held at Schloss Mickeln, Diisseldorf, November 16-21, 1987. In 1982 Tsfasman, Vladut and Zink, using algebraic geometry and ideas of Goppa, constructed a seqeunce of codes that exceed the Gilbert-Varshamov bound. The result was considered sensational. Furthermore, it was surprising to see these unrelated areas of mathematics collaborating. The aim of this course is to give an introduction to coding theory and to sketch the ideas of algebraic geometry that led to the new result. Finally, a number of applications of these methods of algebraic geometry to coding theory are given. Since this is a new area, there are presently no references where one can find a more extensive treatment of all the material. However, both for algebraic geometry and for coding theory excellent textbooks are available. The combination ofthe two subjects can only be found in a number ofsurvey papers. A book by C. Moreno with a complete treatment of this area is in preparation. We hope that these notes will stimulate further research and collaboration of algebraic geometers and coding theorists. G. van der Geer, J.H. van Lint Introduction to CodingTheory and Algebraic Geometry Partl -- CodingTheory Jacobus H. vanLint 11 1. Finite fields In this chapter we collect (without proof) the facts from the theory of finite fields that we shall need in this course
MDS Codes, Algebraic Geometric Codes and Automorphism Group of Function Fields CRC Press
Algebraic Geometry Codes: Advanced Chapters is devoted to the theory of algebraic geometry codes, a subject related to local_libraryBook Catalogseveral domains of mathematics. On one hand, it involves such classical areas as algebraic geometry and number theory; on the other, it is

connected to information transmission theory, combinatorics, finite geometries, dense packings, and so on. The book gives a unique perspective on the subject. Whereas most books on coding theory start with elementary concepts and then develop them in the framework of coding theory itself within, this book systematically presents meaningful and important connections of coding theory with algebraic geometry and number theory. Among many topics treated in the book, the following should be mentioned: curves with many points over finite fields, class field theory, asymptotic theory of global fields, decoding, sphere packing, codes from multi-dimensional varieties, and applications of algebraic geometry codes. The book is the natural continuation of Algebraic Geometric Codes: Basic Notions by the same authors. The concise exposition of the first volume is included as an appendix.