Introduction To Cyclotomic Fields Graduate Texts I

DANIKA KNOX

Official Gazette Springer
A description of 148 algorithms fundamental to number-theoretic computations, in particular for computations related to algebraic number theory, elliptic curves, primality testing and factoring. The first seven chapters guide readers to the heart of current research in computational algebraic number theory, including recent algorithms for computing class groups and units, as well as elliptic curve computations, while the last three chapters survey factoring and primality testing methods, including a detailed description of the number field sieve algorithm. The whole is rounded off with a description of available computer packages and some useful tables, backed by numerous exercises. Written by an authority in the field, and one with great practical and teaching experience, this is certain to become the standard and indispensable reference on the subject.
Canadian Journal of Mathematics Birkhäuser
This book contains a detailed account of the result of the author's recent Annals paper and JAMS paper on arithmetic invariant, including μ-invariant, L-invariant, and similar topics. This book can be regarded as an introductory text to the author's previous book p-Adic Automorphic Forms on Shimura Varieties. Written as a down-to-earth introduction to Shimura varieties, this text includes many examples and applications of the theory that provide motivation for the reader. Since it is limited to modular curves and the corresponding Shimura varieties, this book is not only a great resource for experts in the field, but it is also accessible to advanced graduate students studying number theory. Key topics include non-triviality of arithmetic invariants and special values of L-functions; elliptic curves over complex and p-adic fields; Hecke algebras; scheme theory; elliptic and modular curves over rings; and Shimura curves.
Nonlinear Analysis Princeton University Press
4e de couverture : "These proceedings contain most of the contributions to the Göttingen-Jerusalem Conference 2008 on "Symmetries in Algebra and Number Theory" including three addresses given at the conference opening, and two contributions to the Satellite Conference "On the Legacy of Hermann Weyl". The contributions are survey articles or report on recent work by the authors, for exemple new results on the famous Leopoldt conjecture."
Diophantine Approximation Springer Science & Business Media
This volume contains 21 research and survey papers on recent developments in the field of diophantine approximation, which are based on lectures given at a conference at the Erwin Schrödinger-Institute (Vienna, 2003). The articles are either in the spirit of more classical diophantine analysis or of a geometric or combinatorial flavor. Several articles deal with estimates for the number of solutions of diophantine equations as well as with congruences and polynomials.

Algorithmic Number Theory American Mathematical Soc.

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.

Algebraic Number Theory American Mathematical Soc.

This is the fifth conference in a bi-annual series, following conferences in Besancon, Limoges, Irsee and Toronto. The meeting aims to bring together different strands of research in and closely related to the area of Iwasawa theory. During the week before the conference in a kind of summer school a series of preparatory lectures for young mathematicians was provided as an introduction to Iwasawa theory. Iwasawa theory is a modern and powerful branch of number theory and can be traced back to the Japanese mathematician Kenkichi Iwasawa, who introduced the systematic study of Z_p-extensions and p-adic L-functions, concentrating on the case of ideal class groups. Later this would be generalized to elliptic curves. Over the last few decades considerable progress has been made in automorphic Iwasawa theory, e.g. the proof of the Main Conjecture for GL(2) by Kato and Skinner & Urban. Techniques such as Hida's theory of p-adic modular forms and big Galois representations play a crucial part. Also a noncommutative Iwasawa theory of arbitrary p-adic Lie extensions has been developed. This volume aims to present a snapshot of the state of art of Iwasawa theory as of 2012. In particular it offers an introduction to Iwasawa theory (based on a preparatory course by Chris Wuthrich) and a survey of the proof of Skinner & Urban (based on a lecture course by Xin Wan).

Characters and Cyclotomic Fields in Finite Geometry World Scientific

This book constitutes the refereed post-conference proceedings of the Second International Algorithmic Number Theory Symposium, ANTS-II, held in Talence, France in May 1996. The 35 revised full papers included in the book were selected from a variety of submissions. They cover a broad spectrum of topics and report state-of-the-art research results in computational number theory and complexity theory. Among the issues addressed are number fields computation, Abelian varieties, factoring algorithms, finite fields, elliptic curves, algorithm complexity, lattice theory, and coding.

Irregularities in the Distribution of Prime Numbers Springer Science & Business Media

The aim of cryptography is to design primitives and protocols that withstand adversarial behavior. Information theoretic cryptography, how-so-ever desirable, is extremely restrictive and most non-trivial cryptographic tasks are known to be information theoretically impossible. In order to realize sophisticated cryptographic primitives, we forgo information theoretic security and assume limitations on what can be efficiently computed. In other words we attempt to build secure systems conditioned on some computational intractability assumption such as factoring, discrete log, decisional Diffie-Hellman, learning with errors, and many more. In this work, based on the 2013 ACM Doctoral Dissertation Award-winning thesis, we put forth new plausible lattice-based constructions with properties that approximate the sought after multilinear maps. The multilinear analog of the decision Diffie-Hellman problem appears to be hard in our construction, and this allows for their use in cryptography. These constructions open doors to providing solutions to a number of important open problems.

p-Adic Automorphic Forms on Shimura Varieties Springer Science & Business Media

Global class field theory is a major achievement of algebraic number theory based on the functorial properties of the reciprocity map and the existence theorem. This book explores the consequences and the practical use of these results in detailed studies and illustrations of classical subjects. In the corrected second printing 2005, the author improves many details all through the book.

Group Rings and Class Groups Springer Science & Business Media

This monograph contributes to the existence theory of difference sets, cyclic irreducible codes and similar objects. The new method of field descent for cyclotomic integers of presribed absolute value is developed. Applications include the first substantial progress towards the Circulant Hadamard Matrix Conjecture and Ryser`s conjecture since decades. It is shown that there is no Barker sequence of length l with 13

Number Theory in Function Fields Princeton University Press

The first part of the book centers around the isomorphism problem for finite groups; i.e. which properties of the finite group G can be determined by the integral group ring ZZG ? The authors have tried to present the results more or less selfcontained and in as much generality as possible concerning the ring of coefficients. In the first section, the class sum correspondence and some related results are derived. This part is the proof of the subgroup rigidity theorem (Scott - Roggenkamp; Weiss) which says that a finite subgroup of the p-adic integral group ring of a finite p-group is conjugate to a subgroup of the finite group. A counterexample to the conjecture of Zassenhaus that group basis are rationally conjugate, is presented in the semilocal situation (Scott - Roggenkamp). To this end, an extended version of Clifford theory for p-adic integral group rings is presented. Moreover, several examples are given to demonstrate the complexity of the isomorphism problem. The second part of the book is concerned with various aspects of the structure of rings of integers as Galois modules. It begins with a brief overview of major results in the area; thereafter the majority of the text focuses on the use of the theory of Hopf algebras. It begins with a thorough and detailed treatment of the required foundational material and concludes with new and interesting applications to cyclotomic theory and to elliptic curves with complex multiplication. Examples are used throughout both for motivation, and also to illustrate new ideas.

Algebraic K-Theory and Its Applications Oxford University Press

Describing the applications found for the Wiles and Taylor technique, this book generalizes the deformation theoretic techniques of Wiles-Taylor to Hilbert modular forms (following Fujiwara's treatment), and also discusses applications found by the author.

Quaternion Algebras Springer Nature

Class field theory brings together the quadratic and higher reciprocity laws of Gauss, Legendre, and others, and vastly generalizes them. This book provides an accessible introduction to class field theory. It takes a traditional approach in that it attempts to present the material using the original techniques of proof, but in a fashion which is cleaner and more streamlined than most other books on this topic. It could be used for a graduate course on algebraic number theory, as well as for students who are interested in self-study. The book has been class-tested, and the author has included lots of challenging exercises throughout the text.

Class Field Theory Springer

This open access textbook presents a comprehensive treatment of the arithmetic theory of quaternion algebras and orders, a subject with applications in diverse areas of mathematics. Written to be accessible and approachable to the graduate student reader, this text collects and synthesizes results from across the literature. Numerous pathways offer explorations in many different directions, while the unified treatment makes this book an essential reference for students and researchers alike. Divided into five parts, the book begins with a basic introduction to the noncommutative algebra underlying the theory of quaternion algebras over fields, including the relationship to quadratic forms. An in-depth exploration of the arithmetic of quaternion algebras and orders follows. The third part considers analytic aspects, starting with zeta functions and then passing to an idelic approach, offering a pathway from local to global that includes strong approximation. Applications of unit groups of quaternion orders to hyperbolic geometry and low-dimensional topology follow, relating geometric and topological properties to arithmetic invariants. Arithmetic geometry completes the volume, including quaternionic aspects of modular forms, supersingular elliptic curves, and the moduli of QM abelian surfaces. Quaternion Algebras encompasses a vast wealth of knowledge at the intersection of many fields. Graduate students interested in algebra, geometry, and number theory will appreciate the many avenues and connections to be explored. Instructors will find numerous options for constructing introductory and advanced courses, while researchers will value the all-embracing treatment. Readers are assumed to have some familiarity with algebraic number theory and commutative algebra, as well as the fundamentals of linear algebra, topology, and complex analysis. More advanced topics call upon additional background, as noted, though essential concepts and motivation are recapped throughout.

Number Theory Springer

Kummer's work on cyclotomic fields paved the way for the development of algebraic number theory in general by Dedekind, Weber, Hensel, Hilbert, Takagi, Artin and others. However, the success of this general theory has tended to obscure special facts proved by Kummer about cyclotomic fields which lie deeper than the general theory. For a long period in the 20th century this aspect of Kummer's work seems to have been largely forgotten, except for a few papers, among which are those by Pollaczek [Po], Artin-Hasse [A-H] and Vandiver [Va]. In the mid 1950's, the theory of cyclotomic fields was taken up again by Iwasawa and Leopoldt. Iwasawa viewed cyclotomic fields as being analogues for number fields of the constant field extensions of algebraic geometry, and wrote a great sequence of papers investigating towers of cyclotomic fields, and more generally, Galois extensions of number fields whose Galois group is isomorphic to the additive group of p-adic integers. Leopoldt concentrated on a fixed cyclotomic field, and established various p-adic analogues of the classical complex analytic class number formulas. In particular, this led him to introduce, with Kubota, p-adic analogues of the complex L-functions attached to cyclotomic extensions of the rationals. Finally, in the late 1960's, Iwasawa [Iw 11] made the fundamental discovery that there was a close connection between his work on towers of cyclotomic fields and these p-adic L-functions of Leopoldt - Kubota.

Introduction to Cyclotomic Fields American Mathematical Soc.

Algebraic K-Theory is crucial in many areas of modern mathematics, especially algebraic topology, number theory, algebraic geometry, and operator theory. This text is designed to help graduate students in other areas learn the basics of K-Theory and get a feel for its many applications. Topics include algebraic topology, homological algebra, algebraic number theory, and an introduction to cyclic homology and its interrelationship with K-Theory.

Introduction to p-adic Analytic Number Theory Springer Science & Business Media

This book is an elementary introduction to p-adic analysis from the number theory perspective. With over 100 exercises included, it will acquaint the non-expert to the basic ideas of the theory and encourage the novice to enter this fertile field of research. The main focus of the book is the study of p-adic L-functions and their analytic properties. It begins with a basic introduction to Bernoulli numbers and continues with establishing the Kummer congruences. These congruences are then used to construct the p-adic analog of the Riemann zeta function and p-adic analogs of Dirichlet's L-functions. Featured is a chapter on how to apply the theory of Newton polygons to determine Galois groups of polynomials over the rational number field. As motivation for further study, the final chapter introduces Iwasawa theory.

Cyclotomic Fields and Zeta Values Springer Science & Business Media

This volume presents research and expository papers highlighting the vibrant and fascinating study of irregularities in the distribution of primes. Written by an international group of experts, contributions present a self-contained yet unified exploration of a rapidly progressing area. Emphasis is given to the research inspired by Maier's matrix method, which established a newfound understanding of the distribution of primes. Additionally, the book provides an historical overview of a large body of research in analytic number theory and approximation theory. The papers published within are intended as reference tools for graduate students and researchers in mathematics.

Euler Systems Springer Science & Business Media

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.

Symmetries in Algebra and Number Theory (SANT) Springer Science & Business Media

This book is the first to provide a comprehensive and elementary account of the new Iwasawa theory innovated via the deformation theory of modular forms and Galois representations. The deformation theory of modular forms is developed by generalizing the cohomological approach discovered in the author's 2019 AMS Leroy P Steele Prize-winning article without using much algebraic geometry.Starting with a description of Iwasawa's classical results on his proof of the main conjecture under the Kummer-Vandiver conjecture (which proves cyclicity of his Iwasawa module more than just proving his main conjecture), we describe a generalization of the method proving cyclicity to the adjoint Selmer group of every ordinary deformation of a two-dimensional Artin Galois representation.The fundamentals in the first five chapters are as follows:Many open problems are presented to stimulate young researchers pursuing their field of study.