Algebraic Geometry And Arithmetic Curves By Qing Liu

Algebraic Geometry and Arithmetic CurvesArithmetic GeometryAlgebraic Geometry and Commutative AlgebraModular Forms and Fermat's Last TheoremUndergraduate Algebraic GeometryAlgebraic GeometryRational Points on VarietiesNumber Theory in Function FieldsAlgebraic GeometryNumber Theory and Algebraic GeometryArithmetic of Algebraic CurvesArakelov GeometryAlgebra, Arithmetic, and GeometryDiophantine GeometryAlgebraic Curves Over Finite FieldsBirational Geometry, Rational Curves, and ArithmeticGeometry of Algebraic CurvesAlgebraic CurvesElliptic CurvesAdvanced Topics in the Arithmetic of Elliptic CurvesAlgebraic Geometry over the Complex NumbersArithmetic Noncommutative GeometryArithmetic Algebraic GeometryAlgebraic GeometryConjectures in Arithmetic Algebraic GeometryAlgebraic Curves and CryptographyAlgebraic Geometry and Arithmetic CurvesThe Geometry of SchemesNumber Theory and Geometry: An Introduction to Arithmetic GeometryAlgebraic Geometry I: SchemesGalois Representations in Arithmetic Algebraic GeometryPlane Algebraic CurvesAlgebraic Geometry and Arithmetic CurvesAlgebraic GeometryAlgebraic Curves and Their ApplicationsThe Arithmetic of Elliptic CurvesAn Invitation to Arithmetic GeometryAlgebraic Curves in CryptographyIntegrable Systems and Algebraic GeometryArithmetic Algebraic Geometry

Algebraic Geometry and Arithmetic Curves

Grothendieck's beautiful theory of schemes permeates modern algebraic geometry and underlies its applications to number theory, physics, and applied mathematics. This simple account of that theory emphasizes and explains the universal geometric concepts behind the definitions. In the book, concepts are illustrated with fundamental examples, and explicit calculations show how the constructions of scheme theory are carried out in practice.

Arithmetic Geometry

Algebraic geometry is a fascinating branch of mathematics that combines methods from both, algebra and geometry. It transcends the limited scope of pure algebra by means of geometric construction principles. Moreover, Grothendieck's schemes invented in the late 1950s allowed the application of algebraic-geometric methods in fields that formerly seemed to be far away from geometry, like algebraic number theory. The new techniques paved the way to spectacular progress such as the proof of Fermat's Last Theorem by Wiles and Taylor. The scheme-theoretic approach to algebraic geometry is explained for non-experts. More advanced readers can use the book to broaden their view on the subject. A separate part deals with the necessary prerequisites from commutative algebra. On a whole, the book provides a very accessible and self-contained introduction to algebraic geometry, up to a quite advanced level. Every chapter of the book is preceded by a motivating introduction with an informal discussion of the contents. Typical examples and an abundance of exercises illustrate each section. This way the book is an excellent solution for learning by yourself or for complementing knowledge that is already present. It can equally be used as a convenient source for courses and seminars or as supplemental literature.

Algebraic Geometry and Commutative Algebra

This book features recent developments in a rapidly growing area at the interface of higher-dimensional birational geometry and arithmetic geometry. It focuses on the geometry of spaces of rational curves, with an emphasis on applications to arithmetic questions. Classically, arithmetic is the study of rational or integral solutions of diophantine equations and geometry is the study of lines and conics. From the modern standpoint, arithmetic is the study of rational and integral points on algebraic varieties over nonclosed fields. A major insight of the 20th century was that arithmetic properties of an algebraic variety are tightly linked to the geometry of rational curves on the variety and how they vary in families. This collection of solicited survey and research papers is intended to serve as an introduction for graduate students and researchers interested in entering the field, and as a source of reference for experts working on related problems. Topics that will be addressed include: birational properties such as rationality, unirationality, and rational connectedness, existence of rational curves in prescribed homology classes, cones of rational curves on rationally connected and Calabi-Yau varieties, as well as related questions within the framework of the Minimal Model Program.

Modular Forms and Fermat’s Last Theorem

Undergraduate Algebraic Geometry

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.

Algebraic Geometry

In recent years there has been enormous activity in the theory of algebraic curves.

Many long-standing problems have been solved using the general techniques developed in algebraic geometry during the 1950's and 1960's. Additionally, unexpected and deep connections between algebraic curves and differential equations have been uncovered, and these in turn shed light on other classical problems in curve theory. It seems fair to say that the theory of algebraic curves looks completely different now from how it appeared 15 years ago; in particular, our current state of knowledge repre sents a significant advance beyond the legacy left by the classical geometers such as Noether, Castelnuovo, Enriques, and Severi. These books give a presentation of one of the central areas of this recent activity; namely, the study of linear series on both a fixed curve (Volume I) and on a variable curve (Volume II). Our goal is to give a comprehensive and self-contained account of the extrinsic geometry of algebraic curves, which in our opinion constitutes the main geometric core of the recent advances in curve theory. Along the way we shall, of course, discuss appli cations of the theory of linear series to a number of classical topics (e.g., the geometry of the Riemann theta divisor) as well as to some of the current research (e.g., the Kodaira dimension of the moduli space of curves).

Rational Points on Varieties

In the early 1980's, stimulated by work of Bloch and Deligne, Beilinson stated some intriguing conjectures on special values of L-functions of algebraic varieties defined over number fields. Roughly speaking these special values are determinants of higher regulator maps relating the higher algebraic K-groups of the variety to its cohomology. In this respect, higher algebraic K-theory is believed to provide a universal, motivic cohomology theory and the regulator maps are determined by Chern characters from higher algebraic K-theory to any other suitable cohomology theory. Also, Beilinson stated a generalized Hodge conjecture. This book provides an introduction to and a survey of Beilinson's conjectures and an introduction to Jannsen's work with respect to the Hodge and Tate conjectures. It addresses mathematicians with some knowledge of algebraic number theory, elliptic curves and algebraic K-theory.

Number Theory in Function Fields

This book introduces the reader to modern algebraic geometry. It presents Grothendieck's technically demanding language of schemes that is the basis of the most important developments in the last fifty years within this area. A systematic treatment and motivation of the theory is emphasized, using concrete examples to illustrate its usefulness. Several examples from the realm of Hilbert modular surfaces and of determinantal varieties are used methodically to discuss the covered techniques. Thus the reader experiences that the further development of the theory yields an ever better understanding of these fascinating objects. The text is complemented by many exercises that serve to check the comprehension of the text, treat further examples, or give an outlook on further results. The volume at hand is an introduction to schemes. To get startet, it requires only basic knowledge in abstract algebra and topology. Essential facts from commutative algebra are assembled in an appendix. It will be complemented by a second volume on the cohomology of schemes.

Algebraic Geometry

Conference proceedings based on the 1996 LMS Durham Symposium 'Galois representations in arithmetic algebraic geometry'.

Number Theory and Algebraic Geometry

This is an introduction to diophantine geometry at the advanced graduate level. The book contains a proof of the Mordell conjecture which will make it quite attractive to graduate students and professional mathematicians. In each part of the book, the reader will find numerous exercises.

Arithmetic of Algebraic Curves

Arithmetic algebraic geometry is in a fascinating stage of growth, providing a rich variety of applications of new tools to both old and new problems. Representative of these recent developments is the notion of Arakelov geometry, a way of "completing" a variety over the ring of integers of a number field by adding fibres over the Archimedean places. Another is the appearance of the relations between arithmetic geometry and Nevanlinna theory, or more precisely between diophantine approximation theory and the value distribution theory of holomorphic maps. Research mathematicians and graduate students in algebraic geometry and number theory will find a valuable and lively view of the field in this state-of-the-art selection.

Arakelov Geometry

Geometry and the theory of numbers are as old as some of the oldest historical records of humanity. Ever since antiquity, mathematicians have discovered many beautiful interactions between the two subjects and recorded them in such classical texts as Euclid's Elements and Diophantus's Arithmetica. Nowadays, the field of mathematics that studies the interactions between number theory and algebraic geometry is known as arithmetic geometry. This book is an introduction to number theory and arithmetic geometry, and the goal of the text is to use geometry as the motivation to prove the main theorems in the book. For example, the fundamental theorem of arithmetic is a consequence of the tools we develop in order to find all the integral points on a line in the plane. Similarly, Gauss's law of quadratic reciprocity and the theory of continued fractions naturally arise when we attempt to determine the integral points on a curve in the plane given by a quadratic polynomial equation. After an introduction to the theory of diophantine equations, the rest of the book is structured in three acts that correspond to the study of the integral and rational solutions of linear, quadratic, and cubic curves, respectively. This book describes many applications including modern applications in cryptography; it also presents some recent results in arithmetic geometry. With many exercises, this book can be used as a text for a first course in number theory or for a subsequent course on arithmetic (or diophantine) geometry at the junior-senior level.

Algebra, Arithmetic, and Geometry

This volume honors Sir Peter Swinnerton-Dyer's mathematical career spanning more than 60 years' of amazing creativity in number theory and algebraic geometry.

Diophantine Geometry

Algebraic Curves Over Finite Fields

The main goal of this book is to present the so-called birational Arakelov geometry, which can be viewed as an arithmetic analog of the classical birational geometry, i.e., the study of big linear series on algebraic varieties. After explaining classical results about the geometry of numbers, the author starts with Arakelov geometry for arithmetic curves, and continues with Arakelov geometry of arithmetic surfaces and higher-dimensional varieties. The book includes such fundamental results as arithmetic Hilbert-Samuel formula, arithmetic Nakai-Moishezon criterion, arithmetic Bogomolov inequality, the existence of small sections, the continuity of arithmetic volume function, the Lang-Bogomolov conjecture and so on. In addition, the author presents, with full details, the proof of Faltings' Riemann-Roch theorem. Prerequisites for reading this book are the basic results of algebraic geometry and the language of schemes.

Birational Geometry, Rational Curves, and Arithmetic

This book introduces the reader to modern algebraic geometry. It presents Grothendieck's technically demanding language of schemes that is the basis of the most important developments in the last fifty years within this area. A systematic treatment and motivation of the theory is emphasized, using concrete examples to illustrate its usefulness. Several examples from the realm of Hilbert modular surfaces and of determinantal varieties are used methodically to discuss the covered techniques. Thus the reader experiences that the further development of the theory yields an ever better understanding of these fascinating objects. The text is complemented by many exercises that serve to check the comprehension of the text, treat further examples, or give an outlook on further results. The volume at hand is an introduction to schemes. To get startet, it requires only basic knowledge in abstract algebra and topology. Essential facts from commutative algebra are assembled in an appendix. It will be complemented by a second volume on the cohomology of schemes.

Geometry of Algebraic Curves

An introductory 1997 account in the style of the original discoverers, treating the fundamental themes even-handedly.

Algebraic Curves

Elliptic Curves

In the introduction to the first volume of The Arithmetic of Elliptic Curves (Springer-Verlag, 1986), I observed that "the theory of elliptic curves is rich, varied, and amazingly vast," and as a consequence, "many important topics had to be omitted." I included a brief introduction to ten additional topics as an appendix to the first volume, with the tacit understanding that eventually there might be a second volume containing the details. You are now holding that second volume. it turned out that even those ten topics would not fit Unfortunately, into a single book, so I was forced to make some choices. The following material is covered in this book: I. Elliptic and modular functions for the full modular group. II. Elliptic curves with complex multiplication. III. Elliptic surfaces and specialization theorems. IV. Neron models, Kodaira-Neron classification of special fibers, Tate's algorithm, and Ogg's conductor-discriminant formula. V. Tate's theory of q-curves over p-adic fields. VI. Neron's theory of canonical local height functions.

Advanced Topics in the Arithmetic of Elliptic Curves

This is a relatively fast paced graduate level introduction to complex algebraic geometry, from the basics to the frontier of the subject. It covers sheaf theory, cohomology, some Hodge theory, as well as some of the more algebraic aspects of algebraic geometry. The author frequently refers the reader if the treatment of a certain topic is readily available elsewhere but goes into considerable detail on topics for which his treatment puts a twist or a more transparent viewpoint. His cases of exploration and are chosen very carefully and deliberately. The textbook achieves its purpose of taking new students of complex algebraic geometry through this a deep yet broad introduction to a vast subject, eventually bringing them to the forefront of the topic via a non-intimidating style.

Algebraic Geometry over the Complex Numbers

Author S.A. Stepanov thoroughly investigates the current state of the theory of Diophantine equations and its related methods. Discussions focus on arithmetic, algebraic-geometric, and logical aspects of the problem. Designed for students as well as researchers, the book includes over 250 excercises accompanied by hints, instructions, and references. Written in a clear manner, this text does not require readers to have special knowledge of modern methods of algebraic geometry.

Arithmetic Noncommutative Geometry

EMAlgebra, Arithmetic, and Geometry: In Honor of Yu. I. ManinEM consists of invited expository and research articles on new developments arising from Manin's outstanding contributions to mathematics.

Arithmetic Algebraic Geometry

This book is a general introduction to the theory of schemes, followed by applications to arithmetic surfaces and to the theory of reduction of algebraic curves. The first part introduces basic objects such as schemes, morphisms, base change, local properties (normality, regularity, Zariski's Main Theorem). This is followed by the more global aspect: coherent sheaves and a finiteness theorem for their cohomology groups. Then follows a chapter on sheaves of differentials, dualizing sheaves, and Grothendieck's duality theory. The first part ends with the theorem of Riemann-Roch and its application to the study of smooth projective curves over a field. Singular curves are treated through a detailed study of the Picard group. The second part starts with blowing-ups and desingularisation (embedded or not) of fibered surfaces over a Dedekind ring that leads on to intersection theory on arithmetic surfaces. Castelnuovo's criterion is proved and also the existence of the minimal regular model. This leads to the study of reduction of algebraic curves. The case of elliptic curves is studied in detail. The book concludes with the funadmental theorem of stable reduction of Deligne-Mumford. The book is essentially self-contained, including the necessary material on commutative algebra. The prerequisites are therefore few, and the book should suit a graduate student. It contains many examples and nearly 600 exercises.

Algebraic Geometry

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

Conjectures in Arithmetic Algebraic Geometry

Extremely carefully written, masterfully thought out, and skillfully arranged introduction to the arithmetic of algebraic curves, on the one hand, and to the algebro-geometric aspects of number theory, on the other hand. an excellent guide for beginners in arithmetic geometry, just as an interesting reference and methodical inspiration for teachers of the subject a highly welcome addition to the existing literature. --Zentralblatt MATH The interaction between number theory and algebraic geometry has been especially fruitful. In this volume, the author gives a unified presentation of some of the basic tools and concepts in number theory, commutative algebra, and algebraic geometry, and for the first time in a book at this level, brings out the deep analogies between them. The geometric viewpoint is stressed throughout the book. Extensive examples are given to illustrate each new concept, and many interesting exercises are given at the end of each chapter. Most of the important results in the one-dimensional case are proved, including Bombieri's proof of the Riemann Hypothesis for curves over a finite field. While the book is not intended to be an introduction to schemes, the author indicates how many of the geometric notions introduced in the book relate to schemes, which will aid the reader who goes to the next level of this rich subject.

Algebraic Curves and Cryptography

Arithmetic noncommutative geometry denotes the use of ideas and tools from the field of noncommutative geometry, to address questions and reinterpret in a new perspective results and constructions from number theory and arithmetic algebraic geometry. This general philosophy is applied to the geometry and arithmetic of modular curves and to the fibers at archimedean places of arithmetic surfaces and varieties. The main reason why noncommutative geometry can be expected to say something about topics of arithmetic interest lies in the fact that it provides the right framework in which the tools of geometry continue to make sense on spaces that are very singular and apparently very far from the world of algebraic varieties. This provides a way of refining the boundary structure of certain classes of spaces that arise in the context of arithmetic geometry, such as moduli spaces (of which modular curves are the simplest case) or arithmetic varieties (completed by suitable ``fibers at infinity''), by adding boundaries that are invisible to algebraic geometry, such as degenerations of elliptic curves to noncommutative tori. The text of the book is organized around series of invited lectures delivered by the author at various universities, and the results presented are based on work of the author in collaboration with Alain Connes, Katia Consani, Yuri Manin, and Niranjan Ramachandran.

Algebraic Geometry and Arithmetic Curves

The theory of elliptic curves is distinguished by its long history and by the diversity of the methods that have been used in its study. This book treats the arithmetic approach in its modern formulation, through the use of basic algebraic number theory and algebraic geometry. Following a brief discussion of the necessary algebro-geometric results, the book proceeds with an exposition of the geometry and the formal group of elliptic curves, elliptic curves over finite fields, the complex numbers, local fields, and global fields. Final chapters deal with integral and rational points, including Siegels theorem and explicit computations for the curve Y = X + DX, while three appendices conclude the whole: Elliptic Curves in Characteristics 2 and 3, Group Cohomology, and an overview of more advanced topics.

The Geometry of Schemes

This volume contains a collection of papers on algebraic curves and their applications. While algebraic curves traditionally have provided a path toward modern algebraic geometry, they also provide many applications in number theory, computer security and cryptography, coding theory, differential equations, and more. Papers cover topics such as the rational torsion points of elliptic curves, arithmetic statistics in the moduli space of curves, combinatorial descriptions of semistable hyperelliptic curves over local fields, heights on weighted projective spaces, automorphism groups of curves, hyperelliptic curves, dessins d'enfants, applications to Painlevé equations, descent on real algebraic varieties, quadratic residue codes based on hyperelliptic curves, and Abelian varieties and cryptography. This book will be a valuable resource for people interested in algebraic curves and their connections to other branches of mathematics.

Number Theory and Geometry: An Introduction to Arithmetic Geometry

This book provides an introduction to abstract algebraic geometry. It includes more than 400 exercises that offer specific examples as well as more specialized topics. From the reviews: "Enables the reader to make the drastic transition between the basic, intuitive questions about affine and projective varieties with which the subject begins, and the elaborate general methodology of schemes and cohomology employed currently to answer these questions." --MATHEMATICAL REVIEWS

Algebraic Geometry I: Schemes

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

Galois Representations in Arithmetic Algebraic Geometry

This book offers a concise yet thorough introduction to the notion of moduli spaces of complex algebraic curves. Over the last few decades, this notion has become central not only in algebraic geometry, but in mathematical physics, including string theory, as well. The book begins by studying individual smooth algebraic curves, including the most beautiful ones, before addressing families of curves. Studying families of algebraic curves often proves to be more efficient than studying individual curves: these families and their total spaces can still be smooth, even if there are singular curves among their members. A major discovery of the 20th century, attributed to P. Deligne and D. Mumford, was that curves with only mild singularities form smooth compact moduli spaces. An unexpected byproduct of this discovery was the realization that the analysis of more complex curve singularities is not a necessary step in understanding the geometry of the moduli spaces. The book does not use the sophisticated machinery of modern algebraic geometry, and most classical objects related to curves – such as Jacobian, space of holomorphic differentials, the Riemann-Roch theorem, and Weierstrass points – are treated at a basic level that does not require a profound command of algebraic geometry, but which is sufficient for extending them to vector bundles and other geometric objects associated to moduli spaces.

Nevertheless, it offers clear information on the construction of the moduli spaces, and provides readers with tools for practical operations with this notion. Based on several lecture courses given by the authors at the Independent University of Moscow and Higher School of Economics, the book also includes a wealth of problems, making it suitable not only for individual research, but also as a textbook for undergraduate and graduate coursework

Plane Algebraic Curves

This new-in-paperback edition provides a general introduction to algebraic and arithmetic geometry, starting with the theory of schemes, followed by applications to arithmetic surfaces and to the theory of reduction of algebraic curves. The first part introduces basic objects such as schemes, morphisms, base change, local properties (normality, regularity, Zariski's Main Theorem). This is followed by the more global aspect: coherent sheaves and a finiteness theorem for their cohomology groups. Then follows a chapter on sheaves of differentials, dualizing sheaves, and Grothendieck's duality theory. The first part ends with the theorem of Riemann-Roch and its application to the study of smooth projective curves over a field. Singular curves are treated through a detailed study of the Picard group. The second part starts with blowing-ups and desingularisation (embedded or not) of fibered surfaces over a Dedekind ring that leads on to intersection theory on arithmetic surfaces. Castelnuovo's criterion is proved and also the existence of the minimal regular model. This leads to the study of reduction of algebraic curves. The case of elliptic curves is studied in detail. The book concludes with the fundamental theorem of stable reduction of Deligne-Mumford. This book is essentially self-contained, including the necessary material on commutative algebra. The prerequisites are few, and including many examples and approximately 600 exercises, the book is ideal for graduate students.

Algebraic Geometry and Arithmetic Curves

This short and readable introduction to algebraic geometry will be ideal for all undergraduate mathematicians coming to the subject for the first time.

Algebraic Geometry

It is by now a well-known paradigm that public-key cryptosystems can be built using finite Abelian groups and that algebraic geometry provides a supply of such groups through Abelian varieties over finite fields. Of special interest are the Abelian varieties that are Jacobians of algebraic curves. All of the articles in this volume are centered on the theme of point counting and explicit arithmetic on the Jacobians of curves over finite fields. The topics covered include Schoof's ℓ-adic point counting algorithm, the p-adic algorithms of Kedlaya and Denef-

Vercauteren, explicit arithmetic on the Jacobians of C_{ab} curves and zeta functions. This volume is based on seminars on algebraic curves and cryptography held at the GANITA Lab of the University of Toronto during 2001-2008. The articles are mostly suitable for independent study by graduate students who wish to enter the field, both in terms of introducing basic material as well as guiding them in the literature. The literature in cryptography seems to be growing at an exponential rate. For a new entrant into the subject, navigating through this ocean can seem quite daunting. In this volume, the reader is steered toward a discussion of a few key ideas of the subject, together with some brief guidance for further reading. It is hoped that this approach may render the subject more approachable. Titles in this series are co-published with the Fields Institute for Research in Mathematical Sciences (Toronto, Ontario, Canada).|It is by now a well-known paradigm that public-key cryptosystems can be built using finite Abelian groups and that algebraic geometry provides a supply of such groups through Abelian varieties over finite fields. Of special interest are the Abelian varieties that are Jacobians of algebraic curves. All of the articles in this volume are centered on the theme of point counting and explicit arithmetic on the Jacobians of curves over finite fields. The topics covered include Schoof's ℓ-adic point counting algorithm, the p-adic algorithms of Kedlaya and Denef-Vercauteren, explicit arithmetic on the Jacobians of C_{ab} curves and zeta functions. This volume is based on seminars on algebraic curves and cryptography held at the GANITA Lab of the University of Toronto during 2001-2008. The articles are mostly suitable for independent study by graduate students who wish to enter the field, both in terms of introducing basic material as well as guiding them in the literature. The literature in cryptography seems to be growing at an exponential rate. For a new entrant into the subject, navigating through this ocean can seem quite daunting. In this volume, the reader is steered toward a discussion of a few key ideas of the subject, together with some brief guidance for further reading. It is hoped that this approach may render the subject more approachable. Titles in this series are co-published with the Fields Institute for Research in Mathematical Sciences (Toronto, Ontario, Canada).

Algebraic Curves and Their Applications

This book is based on survey lectures given at the 2006 Clay Summer School on Arithmetic Geometry at the Mathematics Institute of the University of Gottingen. Intended for graduate students and recent Ph.D.'s, this volume will introduce readers to modern techniques and outstanding conjectures at the interface of number theory and algebraic geometry. The main focus is rational points on algebraic varieties over non-algebraically closed fields. Do they exist? If not, can this be proven efficiently and algorithmically? When rational points do exist, are they finite in number and can they be found effectively? When there are infinitely many rational points, how are they distributed? For curves, a cohesive theory addressing these questions has emerged in the last few decades. Highlights include Faltings' finiteness theorem and Wiles's proof of Fermat's Last Theorem. Key techniques are drawn from the theory of elliptic curves, including modular curves and parametrizations, Heegner points, and heights. The arithmetic of higher-dimensional varieties is equally rich, offering a complex interplay of techniques including Shimura varieties, the minimal model program, moduli spaces of curves and maps, deformation theory, Galois cohomology, harmonic analysis, and automorphic functions. However, many foundational questions about the structure of rational points remain open, and research tends to focus on properties of specific classes of varieties.

The Arithmetic of Elliptic Curves

A collection of articles discussing integrable systems and algebraic geometry from leading researchers in the field.

An Invitation to Arithmetic Geometry

This book is motivated by the problem of determining the set of rational points on a variety, but its true goal is to equip readers with a broad range of tools essential for current research in algebraic geometry and number theory. The book is unconventional in that it provides concise accounts of many topics instead of a comprehensive account of just one—this is intentionally designed to bring readers up to speed rapidly. Among the topics included are Brauer groups, faithfully flat descent, algebraic groups, torsors, étale and fppf cohomology, the Weil conjectures, and the Brauer-Manin and descent obstructions. A final chapter applies all these to study the arithmetic of surfaces. The down-to-earth explanations and the over 100 exercises make the book suitable for use as a graduate-level textbook, but even experts will appreciate having a single source covering many aspects of geometry over an unrestricted ground field and containing some material that cannot be found elsewhere.

Algebraic Curves in Cryptography

This book is a general introduction to the theory of schemes, followed by applications to arithmetic surfaces and to the theory of reduction of algebraic curves. The first part introduces basic objects such as schemes, morphisms, base change, local properties (normality, regularity, Zariski's Main Theorem). This is followed by the more global aspect: coherent sheaves and a finiteness theorem for their cohomology groups. Then follows a chapter on sheaves of differentials, dualizing sheaves, and grothendieck's duality theory. The first part ends with the theorem of Riemann-Roch and its application to the study of smooth projective curves over a field. Singular curves are treated through a detailed study of the Picard group. The second part starts with blowing-ups and desingularization (embedded or not) of fibered surfaces over a Dedekind ring that leads on to intersection theory on arithmetic surfaces. Castelnuovo's criterion is proved and also the existence of the minimal regular model. This leads to the study of reduction of algebraic curves. The case of elliptic curves is studied in detail. The book concludes with the fundamental theorem of stable reduction of Deligne-Mumford. The book is essentially self-contained, including the necessary material on commutative algebra. The prerequisites are therefore few, and the book should suit a graduate student. It contains many examples and nearly 600 exercises.

Integrable Systems and Algebraic Geometry

Aimed primarily at graduate students and beginning researchers, this book provides an introduction to algebraic geometry that is particularly suitable for those with no previous contact with the subject; it assumes only the standard background of undergraduate algebra. The book starts with easily-formulated problems with non-trivial solutions and uses these problems to introduce the fundamental tools of modern algebraic geometry: dimension; singularities; sheaves; varieties; and cohomology. A range of exercises is provided for each topic discussed, and a selection of problems and exam papers are collected in an appendix to provide material for further study.

Arithmetic Algebraic Geometry

This volume contains the expanded lectures given at a conference on number theory and arithmetic geometry held at Boston University. It introduces and explains the many ideas and techniques used by Wiles, and to explain how his result can be combined with Ribets theorem and ideas of Frey and Serre to prove Fermats Last Theorem. The book begins with an overview of the complete proof, followed by several introductory chapters surveying the basic theory of elliptic curves, modular functions and curves, Galois cohomology, and finite group schemes. Representation theory, which lies at the core of the proof, is dealt with in a chapter on automorphic representations and the Langlands-Tunnell theorem, and this is followed by in-depth discussions of Serres conjectures, Galois deformations, universal deformation rings, Hecke algebras, and complete intersections. The book concludes by looking both forward and backward, reflecting on the history of the problem, while placing Wiles'theorem into a more general Diophantine context suggesting future applications. Students and professional mathematicians alike will find this an indispensable resource.