Rational Points On Elliptic Curves Undergraduate

Right here, we have countless ebook **rational points on elliptic curves undergraduate** and collections to check out. We additionally find the money for variant types and plus type of the books to browse. The suitable book, fiction, history, novel, scientific research, as competently as various new sorts of books are readily reachable here.

As this rational points on elliptic curves undergraduate, it ends stirring being one of the favored book rational points on elliptic curves undergraduate collections that we have. This is why you remain in the best website to look the incredible book to have.

Rational Points on Elliptic Curves Joseph H. Silverman 2013-04-17 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.

Fermat's Last Theorem Harold M. Edwards 2000-01-14 This introduction to algebraic number theory via the famous problem of "Fermats Last Theorem" follows its historical development, beginning with the work of Fermat and ending with Kummers theory of "ideal" factorization. The more elementary topics, such as Eulers proof of the impossibilty of x+y=z, are treated in an uncomplicated way, and new concepts and techniques are introduced only after having been motivated by specific problems. The book also covers in detail the application of Kummers theory to quadratic integers and relates this to Gauss'theory of binary quadratic forms, an interesting and important connection that is not explored in any other book.

The Arithmetic of Elliptic Curves Joseph H. Silverman 2013-03-09 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.

Number Theory, Analysis and Geometry Dorian Goldfeld 2011-12-21 Serge Lang was an iconic figure in mathematics, both for his own important work and for the indelible impact he left on the field of mathematics, on his students, and on his colleagues. Over the course of his career, Lang traversed a tremendous amount of mathematical ground. As he moved from subject to subject, he found analogies that led to important questions in such areas as number theory, arithmetic geometry, and the theory of negatively curved spaces. Lang's conjectures will keep many mathematicians occupied far into the future. In the spirit of Lang’s vast contribution to mathematics, this memorial volume contains articles by prominent mathematicians in a variety of areas of the field, namely Number Theory, Analysis, and Geometry, representing Lang’s own breadth of interest and impact. A special introduction by John Tate includes a brief and fascinating account of the Serge Lang’s life. This volume's group of 6 editors are also highly prominent mathematicians and were close to Serge Lang, both academically and personally. The volume is suitable to research mathematicians in the areas of Number Theory, Analysis, and Geometry.

Modular Forms, a Computational Approach William A. Stein 2007-02-13 This marvellous and highly original book fills a significant gap in the extensive literature on classical modular forms. This is not just yet another introductory text to this theory, though it could certainly be used as such in conjunction with more traditional treatments. Its novelty lies in its computational emphasis throughout: Stein not only defines what modular forms are, but shows in illuminating detail how one can compute everything about them in practice. This is illustrated throughout the book with examples from his own (entirely free) software package SAGE, which really bring the subject to life while not detracting in any way from its theoretical beauty. The author is the leading expert in computations with modular forms, and what he says on this subject is all tried and tested and based on his extensive experience. As well as being an invaluable companion to those learning the theory in a more traditional way, this book will be a great help to those who wish to use modular forms in applications, such as in the explicit solution of Diophantine equations. There is also a useful Appendix by Gunnells on extensions to more general modular forms, which has enough in it to inspire many PhD theses for years to come. While the book's main readership will be graduate students in number theory, it will also be accessible to advanced undergraduates and useful to both specialists and non-specialists in number theory. --John E. Cremona, University of Nottingham William Stein is an associate professor of mathematics at the University of Washington at Seattle. He earned a PhD in mathematics from UC Berkeley and has held positions at Harvard University and UC San Diego. His current research interests lie in modular forms, elliptic curves, and computational mathematics.

An Invitation to Algebraic Geometry Karen E. Smith 2013-03-09 This is a description of the underlying principles of algebraic geometry, some of its important developments in the twentieth century, and some of the problems that

occupy its practitioners today. It is intended for the working or the aspiring mathematician who is unfamiliar with algebraic geometry but wishes to gain an appreciation of its foundations and its goals with a minimum of prerequisites. Few algebraic prerequisites are presumed beyond a basic course in linear algebra.

Rational Points on Elliptic Curves Joseph H. Silverman 1994-11-18 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.

Elliptic Curves and Their Applications to Cryptography Andreas Enge 2012-12-06 Since their invention in the late seventies, public key cryptosystems have become an indispensable asset in establishing private and secure electronic communication, and this need, given the tremendous growth of the Internet, is likely to continue growing. Elliptic curve cryptosystems represent the state of the art for such systems. Elliptic Curves and Their Applications to Cryptography: An Introduction provides a comprehensive and self-contained introduction to elliptic curves and how they are employed to secure public key cryptosystems. Even though the elegant mathematical theory underlying cryptosystems is considerably more involved than for other systems, this text requires the reader to have only an elementary knowledge of basic algebra. The text nevertheless leads to problems at the forefront of current research, featuring chapters on point counting algorithms and security issues. The Adopted unifying approach treats with equal care elliptic curves over fields of even characteristic, which are especially suited for hardware implementations, and curves over fields of odd characteristic, which have traditionally received more attention. Elliptic Curves and Their Applications: An Introduction has been used successfully for teaching advanced undergraduate courses. It will be of greatest interest to mathematicians, computer scientists, and engineers who are curious about elliptic curve cryptography in practice, without losing the beauty of the underlying mathematics.

Geometry of Algebraic Curves Enrico Arbarello 2011-03-10 The second volume of the Geometry of Algebraic Curves is devoted to the foundations of the theory of moduli of algebraic curves. Its authors are research mathematicians who have actively participated in the development of the Geometry of Algebraic Curves. The subject is an extremely fertile and active one, both within the mathematical community and at the interface with the theoretical physics community. The approach is unique in its blending of algebro-geometric, complex analytic and topological/combinatorial methods. It treats important topics such as Teichmüller theory, the cellular decomposition of moduli and its consequences and the Witten conjecture. The careful and comprehensive presentation of the material is of value to students who wish to learn the subject and to experts as a reference source. The first volume appeared 1985 as

vol. 267 of the same series.

Modern Cryptography and Elliptic Curves: A Beginner's Guide Thomas R. Shemanske 2017-07-31 This book offers the beginning undergraduate student some of the vista of modern mathematics by developing and presenting the tools needed to gain an understanding of the arithmetic of elliptic curves over finite fields and their applications to modern cryptography. This gradual introduction also makes a significant effort to teach students how to produce or discover a proof by presenting mathematics as an exploration, and at the same time, it provides the necessary mathematical underpinnings to investigate the practical and implementation side of elliptic curve cryptography (ECC). Elements of abstract algebra, number theory, and affine and projective geometry are introduced and developed, and their interplay is exploited. Algebra and geometry combine to characterize congruent numbers via rational points on the unit circle, and group law for the set of points on an elliptic curve arises from geometric intuition provided by Bézout's theorem as well as the construction of projective space. The structure of the unit group of the integers modulo a prime explains RSA encryption, Pollard's method of factorization, Diffie–Hellman key exchange, and ElGamal encryption, while the group of points of an elliptic curve over a finite field motivates Lenstra's elliptic curve factorization method and ECC. The only real prerequisite for this book is a course on one-variable calculus; other necessary mathematical topics are introduced on-the-fly. Numerous exercises further guide the exploration.

Number Theory and Geometry: An Introduction to Arithmetic Geometry Álvaro Lozano-Robledo 2019-03-21 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.

Number Theory Revealed: A Masterclass Andrew Granville 2020-09-23 Number Theory

Revealed: A Masterclass acquaints enthusiastic students with the “Queen of Mathematics”. The text offers a fresh take on congruences, power residues, quadratic residues, primes, and Diophantine equations and presents hot topics like cryptography, factoring, and primality testing. Students are also introduced to beautiful enlightening questions like the structure of Pascal's triangle mod p and modern twists on traditional questions like the values represented by binary quadratic forms, the anatomy of integers, and elliptic curves. This Masterclass edition contains many additional chapters and appendices not found in Number Theory Revealed: An Introduction, highlighting beautiful developments and inspiring other subjects in mathematics (like algebra). This allows instructors to tailor a course suited to their own (and their students') interests. There are new yet accessible topics like the curvature of circles in a tiling of a circle by circles, the latest discoveries on gaps between primes, a new proof of Mordell's Theorem for congruent elliptic curves, and a discussion of the abc-conjecture including its proof for polynomials. About the Author: Andrew Granville is the Canada Research Chair in Number Theory at the University of Montreal and professor of mathematics at University College London. He has won several international writing prizes for exposition in mathematics, including the 2008 Chauvenet Prize and the 2019 Halmos-Ford Prize, and is the author of Prime Suspects (Princeton University Press, 2019), a beautifully illustrated graphic novel murder mystery that explores surprising connections between the anatomies of integers and of permutations.

Modular Forms and Fermat’s Last Theorem Gary Cornell 2013-12-01 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.

A First Course in Modular Forms Fred Diamond 2006-03-30 This book introduces the theory of modular forms, from which all rational elliptic curves arise, with an eye toward the Modularity Theorem. Discussion covers elliptic curves as complex tori and as algebraic curves; modular curves as Riemann surfaces and as algebraic curves; Hecke operators and Atkin-Lehner theory; Hecke eigenforms and their arithmetic properties; the Jacobians of modular curves and the Abelian varieties associated to Hecke eigenforms. As it presents these ideas, the book

states the Modularity Theorem in various forms, relating them to each other and touching on their applications to number theory. The authors assume no background in algebraic number theory and algebraic geometry. Exercises are included.

Elliptic Curves (Second Edition) James S Milne 2020-08-20 This book uses the beautiful theory of elliptic curves to introduce the reader to some of the deeper aspects of number theory. It assumes only a knowledge of the basic algebra, complex analysis, and topology usually taught in first-year graduate courses.An elliptic curve is a plane curve defined by a cubic polynomial. Although the problem of finding the rational points on an elliptic curve has fascinated mathematicians since ancient times, it was not until 1922 that Mordell proved that the points form a finitely generated group. There is still no proven algorithm for finding the rank of the group, but in one of the earliest important applications of computers to mathematics, Birch and Swinnerton-Dyer discovered a relation between the rank and the numbers of points on the curve computed modulo a prime. Chapter IV of the book proves Mordell's theorem and explains the conjecture of Birch and Swinnerton-Dyer.Every elliptic curve over the rational numbers has an L-series attached to it.Hasse conjectured that this L-series satisfies a functional equation, and in 1955 Taniyama suggested that Hasse's conjecture could be proved by showing that the L-series arises from a modular form. This was shown to be correct by Wiles (and others) in the 1990s, and, as a consequence, one obtains a proof of Fermat's Last Theorem. Chapter V of the book is devoted to explaining this work.The first three chapters develop the basic theory of elliptic curves.For this edition, the text has been completely revised and updated.

Elliptic Curves Lawrence C. Washington 2008-04-03 Like its bestselling predecessor, Elliptic Curves: Number Theory and Cryptography, Second Edition develops the theory of elliptic curves to provide a basis for both number theoretic and cryptographic applications. With additional exercises, this edition offers more comprehensive coverage of the fundamental theory, techniques, and applications of elliptic curves. New to the Second Edition Chapters on isogenies and hyperelliptic curves A discussion of alternative coordinate systems, such as projective, Jacobian, and Edwards coordinates, along with related computational issues A more complete treatment of the Weil and Tate–Lichtenbaum pairings Doud’s analytic method for computing torsion on elliptic curves over Q An explanation of how to perform calculations with elliptic curves in several popular computer algebra systems Taking a basic approach to elliptic curves, this accessible book prepares readers to tackle more advanced problems in the field. It introduces elliptic curves over finite fields early in the text, before moving on to interesting applications, such as cryptography, factoring, and primality testing. The book also discusses the use of elliptic curves in Fermat’s Last Theorem. Relevant abstract algebra material on group theory and fields can be found in the appendices.

Elliptic Curves Henry McKean 1999-08-13 An introductory 1997 account in the style of the original discoverers, treating the fundamental themes even-

handedly.

Algebraic Curves in Cryptography San Ling 2013-06-13 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

Rational Points on Elliptic Curves Joseph H. Silverman 2015-06-02 The theory of elliptic curves involves a pleasing blend of algebra, geometry, analysis, and number theory. This volume stresses this interplay as it develops the basic theory, thereby providing an opportunity for advanced undergraduates to appreciate the unity of modern mathematics. At the same time, every effort has been made to use only methods and results commonly included in the undergraduate curriculum. This accessibility, the informal writing style, and a wealth of exercises make Rational Points on Elliptic Curves an ideal introduction for students at all levels who are interested in learning about Diophantine equations and arithmetic geometry. Most concretely, an elliptic curve is the set of zeroes of a cubic polynomial in two variables. If the polynomial has rational coefficients, then one can ask for a description of those zeroes whose coordinates are either integers or rational numbers. It is this number theoretic question that is the main subject of Rational Points on Elliptic Curves. Topics covered include the geometry and group structure of elliptic curves, the Nagell–Lutz theorem describing points of finite order, the Mordell–Weil theorem on the finite generation of the group of rational points, the Thue–Siegel theorem on the finiteness of the set of integer points, theorems on counting points with coordinates in finite fields, Lenstra's elliptic curve factorization algorithm, and a discussion of complex multiplication and the Galois representations associated to torsion points. Additional topics new to the second edition include an introduction to elliptic curve cryptography and a brief discussion of the stunning proof of Fermat's Last Theorem by Wiles et al. via the use of elliptic curves.

Rational Points on Varieties Bjorn Poonen 2017-12-13 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.

Advanced Topics in the Arithmetic of Elliptic Curves Joseph H. Silverman 2013-12-01 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.

Undergraduate Algebraic Geometry Miles Reid 1988-12-15 This short and readable introduction to algebraic geometry will be ideal for all undergraduate mathematicians coming to the subject for the first time.

Elliptic Curves. (MN-40) Anthony W. Knapp 2018-06-05 An elliptic curve is a particular kind of cubic equation in two variables whose projective solutions form a group. Modular forms are analytic functions in the upper half plane with certain transformation laws and growth properties. The two subjects--elliptic curves and modular forms--come together in Eichler-Shimura theory, which constructs elliptic curves out of modular forms of a special kind. The converse, that all rational elliptic curves arise this way, is called the Taniyama-Weil Conjecture and is known to imply Fermat's Last Theorem. Elliptic curves and the modeular forms in the Eichler- Shimura theory both have associated L functions, and it is a consequence of the theory that the two kinds of L functions match. The theory covered by Anthony Knapp in this book is, therefore, a window into a broad expanse of mathematics--including class field theory, arithmetic algebraic geometry, and group representations--in which the concidence of L functions relates analysis and algebra in the most fundamental ways. Developing, with many examples, the elementary theory of elliptic curves, the book goes on to the subject of modular forms and the first connections with elliptic curves. The last two chapters concern Eichler-Shimura theory, which establishes a much deeper relationship between the two subjects. No other book in print treats the basic theory of elliptic curves with only undergraduate mathematics, and no other explains Eichler-Shimura theory in such an accessible manner.

Introduction to Elliptic Curves and Modular Forms Neal I. Koblitz 2012-12-06 The theory of elliptic curves and modular forms provides a fruitful meeting ground for such diverse areas as number theory, complex analysis, algebraic geometry, and representation theory. This book starts out with a problem from elementary number theory and proceeds to lead its reader into the modern theory, covering such topics as the Hasse-Weil L-function and the conjecture of

Birch and Swinnerton-Dyer. This new edition details the current state of knowledge of elliptic curves.

LMSST: 24 Lectures on Elliptic Curves J. W. S. Cassels 1991-11-21 A self-contained introductory text for beginning graduate students that is contemporary in approach without ignoring historical matters.

Algorithms for Modular Elliptic Curves Full Canadian Binding J. E. Cremona 1997-05-15 This book presents an extensive set of tables giving information about elliptic curves.

Diophantine Geometry Marc Hindry 2013-12-01 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.

Introduction to Algebraic Geometry Serge Lang 2019-03-20 Rapid, concise, self-contained introduction assumes only familiarity with elementary algebra. Subjects include algebraic varieties; products, projections, and correspondences; normal varieties; differential forms; theory of simple points; algebraic groups; more. 1958 edition.

A Gateway to Number Theory: Applying the Power of Algebraic Curves Keith Kendig 2021-04-23 Challenge: Can you find all the integers a, b, c satisfying 2a2+3b2=5c2? Looks simple, and there are in fact a number of easy solutions. But most of them turn out to be anything but obvious! There are infinitely many possibilities, and as any computer will tell you, each of a, b, c will usually be large. So the challenge remains … Find all integers a a, b, c satisfying 2a2+3b2=5c2 A major advance in number theory means this book can give an easy answer to this and countless similar questions. The idea behind the approach is transforming a degree-two equation in integer variables a, b, c into a plane curve defined by a polynomial. Working with the curve makes obtaining solutions far easier, and the geometric solutions then get translated back into integers. This method morphs hard problems into routine ones and typically requires no more than high school math. (The complete solution to 2a2+3b2=5c2 is included in the book.) In addition to equations of degree two, the book addresses degree-three equations—a branch of number theory that is today something of a cottage industry, and these problems translate into “elliptic curves”. This important part of the book includes many pictures along with the exposition, making the material meaningful and easy to grasp. This book will fit nicely into an introductory course on number theory. In addition, the many solved examples, illustrations, and exercises make self-studying the book an option for students, thus becoming a natural candidate for a capstone course.

Algebraic Number Theory and Fermat's Last Theorem Ian Stewart 2001-12-12 First published in 1979 and written by two distinguished mathematicians with a special gift for exposition, this book is now available in a completely revised

third edition. It reflects the exciting developments in number theory during the past two decades that culminated in the proof of Fermat's Last Theorem. Intended as a upper level textbook, it

Conics and Cubics Robert Bix 2006-07-24 Conics and Cubics offers an accessible and well illustrated introduction to algebraic curves. By classifying irreducible cubics over the real numbers and proving that their points form Abelian groups, the book gives readers easy access to the study of elliptic curves. It includes a simple proof of Bezout’s Theorem on the number of intersections of two curves. The subject area is described by means of concrete and accessible examples. The book is a text for a one-semester course.

Rational Points on Modular Elliptic Curves Henri Darmon 2004 The book surveys some recent developments in the arithmetic of modular elliptic curves. It places a special emphasis on the construction of rational points on elliptic curves, the Birch and Swinnerton-Dyer conjecture, and the crucial role played by modularity in shedding light on these two closely related issues. The main theme of the book is the theory of complex multiplication, Heegner points, and some conjectural variants. The first three chapters introduce the background and prerequisites: elliptic curves, modular forms and the Shimura-Taniyama-Weil conjecture, complex multiplication and the Heegner point construction. The next three chapters introduce variants of modular parametrizations in which modular curves are replaced by Shimura curves attached to certain indefinite quaternion algebras. The main new contributions are found in Chapters 7-9, which survey the author's attempts to extend the theory of Heegner points and complex multiplication to situations where the base field is not a CM field. Chapter 10 explains the proof of Kolyvagin's theorem, which relates Heegner points to the arithmetic of elliptic curves and leads to the so-far best evidence for the Birch and Swinnerton-Dyer conjecture.

Elliptic Tales Avner Ash 2014-10-19 Elliptic Tales describes the latest developments in number theory by looking at one of the most exciting unsolved problems in contemporary mathematics--the Birch and Swinnerton-Dyer Conjecture. The Clay Mathematics Institute is offering a prize of $1 million to anyone who can discover a general solution to the problem. The key to the conjecture lies in elliptic curves, which are cubic equations in two variables. These equations may appear simple, yet they arise from some very deep--and often very mystifying--mathematical ideas. Using only basic algebra and calculus while presenting numerous eye-opening examples, Ash and Gross make these ideas accessible to general readers, and, in the process, venture to the very frontiers of modern mathematics. Along the way, they give an informative and entertaining introduction to some of the most profoundmay appear simple, yet they arise from some very deep--and often very mystifying--mathematical ideas. Using only basic algebra and calculus while presenting numerous eye-opening examples, Ash and Gross make these ideas accessible to general readers, and, in the process, venture to the very frontiers of modern mathematics. Along the way, they give an informative and entertaining introduction to some of the most profound discoveries of the last three centuries in algebraic geometry,

abstract algebra, and number theory. They demonstrate how mathematics grows more abstract to tackle ever more challenging problems, and how each new generation of mathematicians builds on the accomplishments of those who preceded them. Ash and Gross fully explain how the Birch and Swinnerton-Dyer Conjecture sheds light on the number theory of elliptic curves, and how it provides a beautiful and startling connection between two very different objects arising from an elliptic curve, one based on calculus, the other on algebra.

Algebraic Geometry Thomas A. Garrity 2013-02-01 Algebraic Geometry has been at the center of much of mathematics for hundreds of years. It is not an easy field to break into, despite its humble beginnings in the study of circles, ellipses, hyperbolas, and parabolas. This text consists of a series of ex

Elliptic Curves, Modular Forms, and Their L-functions Alvaro Lozano-Robledo 2011 Many problems in number theory have simple statements, but their solutions require a deep understanding of algebra, algebraic geometry, complex analysis, group representations, or a combination of all four. The original simply stated problem can be obscured in the depth of the theory developed to understand it. This book is an introduction to some of these problems, and an overview of the theories used nowadays to attack them, presented so that the number theory is always at the forefront of the discussion. Lozano-Robledo gives an introductory survey of elliptic curves, modular forms, and L-functions. His main goal is to provide the reader with the big picture of the surprising connections among these three families of mathematical objects and their meaning for number theory. As a case in point, Lozano-Robledo explains the modularity theorem and its famous consequence, Fermat's Last Theorem. He also discusses the Birch and Swinnerton-Dyer Conjecture and other modern conjectures. The book begins with some motivating problems and includes numerous concrete examples throughout the text, often involving actual numbers, such as 3, 4, 5, $\frac{3344161}{747348}$, and $\frac{224403517704336969924557513090667486316094847204 1}{8912332268928859588025535178967163570016480830}$. The theories of elliptic curves, modular forms, and L-functions are too vast to be covered in a single volume, and their proofs are outside the scope of the undergraduate curriculum. However, the primary objects of study, the statements of the main theorems, and their corollaries are within the grasp of advanced undergraduates. This book concentrates on motivating the definitions, explaining the statements of the theorems and conjectures, making connections, and providing lots of examples, rather than dwelling on the hard proofs. The book succeeds if, after reading the text, students feel compelled to study elliptic curves and modular forms in all their glory.

The Arithmetic of Elliptic Curves Joseph H. Silverman 2009-04-20 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.

An Introduction to Number Theory G. Everest 2007-05-21 Includes up-to-date material on recent developments and topics of significant interest, such as elliptic functions and the new primality test Selects material from both the algebraic and analytic disciplines, presenting several different proofs of a single result to illustrate the differing viewpoints and give good insight

Elliptic Curves Dale Husemoller 2013-06-29 The book divides naturally into several parts according to the level of the material, the background required of the reader, and the style of presentation with respect to details of proofs. For example, the first part, to Chapter 6, is undergraduate in level, the second part requires a background in Galois theory and the third some complex analysis, while the last parts, from Chapter 12 on, are mostly at graduate level. A general outline ofmuch ofthe material can be found in Tate's colloquium lectures reproduced as an article in Inven tiones [1974]. The first part grew out of Tate's 1961 Haverford Philips Lectures as an attempt to write something for publication c10sely related to the original Tate notes which were more or less taken from the tape recording of the lectures themselves. This inc1udes parts of the Introduction and the first six chapters The aim ofthis part is to prove, by elementary methods, the Mordell theorem on the finite generation of the rational points on elliptic curves defined over the rational numbers. In 1970 Tate teturned to Haverford to give again, in revised form, the originallectures of 1961 and to extend the material so that it would be suitable for publication. This led to a broader plan forthe book.

Mathematics of Public Key Cryptography Steven D. Galbraith 2012-03-15 This advanced graduate textbook gives an authoritative and insightful description of the major ideas and techniques of public key cryptography.

Algebraic Curves over a Finite Field J. W. P. Hirschfeld 2013-03-25 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.