elliptic curves

elliptic curves represent a fundamental concept in modern mathematics, playing a crucial role in number theory, algebraic geometry, and cryptography. These smooth, projective algebraic curves possess fascinating properties that have been extensively studied for their theoretical significance and practical applications. Elliptic curves are defined by cubic equations in two variables with a distinctive structure that allows for a well-defined addition operation on their points, forming an abelian group. This unique group structure underpins their use in cryptography, especially in secure communication protocols like Elliptic Curve Cryptography (ECC). The study of elliptic curves also intersects with famous conjectures and theorems such as Fermat's Last Theorem. This article explores the definition, mathematical properties, applications, and computational techniques related to elliptic curves, providing a comprehensive overview of their importance in contemporary mathematics and technology.

Definition and Mathematical Background of Elliptic Curves

Elliptic curves are algebraic curves defined by cubic equations of the form $y^2 = x^3 + ax + b$, where a and b are constants that satisfy a non-singularity condition. This condition, expressed as $4a^3 + 27b^2 \neq 0$, ensures that the curve has no cusps or self-intersections, thereby making it smooth. These curves are studied over various fields, including real numbers, complex numbers, and finite fields, each context offering unique insights and applications.

Basic Equation and Non-Singularity Condition

The general Weierstrass equation $y^2 = x^3 + ax + b$ defines elliptic curves in two variables. The condition $4a^3 + 27b^2 \neq 0$ guarantees the curve is nonsingular, meaning it has no sharp points or crossings. This smoothness

enables the well-defined geometric and algebraic properties that distinguish elliptic curves from other cubic curves.

Elliptic Curves over Different Fields

Elliptic curves can be studied over real numbers ($\mathbb{R}$), complex numbers ($\mathbb{C}$), rational numbers ($\mathbb{Q}$), and finite fields ($\mathbb{F}_p$). Over the complex numbers, elliptic curves have a rich structure connected to complex tori and modular forms. Over finite fields, elliptic curves become essential in cryptographic systems due to their discrete group properties.

Properties and Group Structure of Elliptic Curves

One of the most remarkable features of elliptic curves is their inherent group structure. The set of points on an elliptic curve, together with a point at infinity, forms an abelian group with a well-defined addition operation. This algebraic structure enables a variety of mathematical and computational applications, particularly in cryptography and number theory.

Addition of Points on Elliptic Curves

The addition operation on elliptic curves is geometrically defined: given two points P and Q on the curve, the line through P and Q intersects the curve at a third point, which is then reflected about the x-axis to yield the sum P + Q. This operation satisfies the group axioms of closure, associativity, identity, and inverses.

Group Law and Its Algebraic Expression

The group law on an elliptic curve can be expressed algebraically through formulas involving the coordinates of points. This algebraic formulation facilitates efficient computation of point addition and doubling, which are critical for cryptographic algorithms relying on elliptic curves.

- Closure: The sum of two points on the curve is also on the curve.
- Associativity: Point addition is associative.
- Identity Element: The point at infinity acts as the identity.
- Inverse Element: Every point has an inverse under addition.

Applications of Elliptic Curves in Cryptography

Elliptic curves have revolutionized cryptography by enabling secure communication methods with smaller key sizes and higher efficiency compared to classical systems such as RSA. Elliptic Curve Cryptography (ECC) leverages the hardness of the Elliptic Curve Discrete Logarithm Problem (ECDLP) to provide robust security.

Elliptic Curve Cryptography (ECC)

ECC uses the group structure of elliptic curves over finite fields to create cryptographic keys. The difficulty of solving the discrete logarithm problem on elliptic curves ensures strong security, making ECC widely adopted in various security protocols, including SSL/TLS, digital signatures, and encryption.

Advantages of ECC over Traditional Cryptosystems

Compared to traditional cryptography methods, ECC offers:

- Smaller key sizes for equivalent security levels
- Faster computations and reduced processing power
- Lower memory requirements, ideal for constrained devices
- Enhanced security against known cryptanalytic attacks

Computational Methods and Algorithms for Elliptic Curves

Efficient computation on elliptic curves is essential for both theoretical research and practical cryptographic implementations. Many algorithms have been developed to perform point addition, multiplication, and other operations with optimized speed and security.

Point Multiplication Techniques

Point multiplication, the repeated addition of a point to itself, is a fundamental operation in elliptic curve algorithms. Methods such as double-and-add, windowed multiplication, and Montgomery ladder improve computational efficiency and resistance to side-channel attacks.

Elliptic Curve Factorization and Primality Testing

Elliptic curves also play a role in integer factorization and primality testing algorithms. The Lenstra Elliptic Curve Factorization method uses properties of elliptic curves to factor large integers, while certain primality tests employ elliptic curve constructions to verify the primality of numbers.

Advanced Topics and Current Research in Elliptic Curves

Research into elliptic curves continues to advance, exploring deep theoretical questions and expanding applications. Connections with modular forms, L-functions, and the Birch and Swinnerton-Dyer conjecture highlight the profound mathematical significance of elliptic curves.

Elliptic Curves and Number Theory

Elliptic curves are central to many problems in number theory, including the proof of Fermat’s Last Theorem by Andrew Wiles. The modularity theorem established that every rational elliptic curve corresponds to a modular form, revealing deep links between different mathematical domains.

Quantum Computing and Elliptic Curves

The advent of quantum computing poses challenges to the security of elliptic curve cryptography. Research is ongoing to develop quantum-resistant algorithms and understand how quantum algorithms may affect the hardness of problems related to elliptic curves.

- Study of rational points and ranks of elliptic curves
- Generalizations to higher-dimensional abelian varieties
- Post-quantum cryptography alternatives
- Algorithmic improvements for large-scale computations

Frequently Asked Questions

What is an elliptic curve in mathematics?

An elliptic curve is a smooth, projective algebraic curve of genus one, with a specified point defined over a field. It is commonly represented by an equation of the form $y^2 = x^3 + ax + b$.

How are elliptic curves used in cryptography?

Elliptic curves are used in cryptography for public-key algorithms, such as Elliptic Curve Cryptography (ECC), which provides similar security to traditional methods with smaller key sizes, improving speed and efficiency.

What is the significance of the group law on elliptic curves?

The group law on elliptic curves defines an addition operation for points on the curve, making the set of points an abelian group. This property is fundamental for cryptographic applications and number theory.

What is the Elliptic Curve Discrete Logarithm Problem (ECDLP)?

ECDLP is the problem of finding an integer k given points P and Q = kP on an elliptic curve. It is computationally hard, which underpins the security of elliptic curve cryptographic systems.

How does elliptic curve cryptography compare to RSA?

Elliptic curve cryptography offers comparable security to RSA but with much smaller key sizes, leading to faster computations, reduced storage, and lower power consumption.

What are some common elliptic curves used in practice?

Common elliptic curves include secp256k1 (used in Bitcoin), NIST P-256, Curve25519, and Ed25519, each chosen for specific security and performance properties.

Can elliptic curves be used over any field?

Elliptic curves can be defined over various fields, including real numbers, complex numbers, finite fields, and p-adic fields. Cryptographic applications typically use elliptic curves over finite fields.

What is the role of elliptic curves in the proof of

Fermat's Last Theorem?

Elliptic curves were central to Andrew Wiles' proof of Fermat's Last Theorem through the modularity theorem, linking elliptic curves over rationals to modular forms.

How does the point at infinity function on an elliptic curve?

The point at infinity acts as the identity element in the elliptic curve group law, analogous to zero in addition, ensuring closure and invertibility of the group operation.

What advancements are being made in post-quantum cryptography involving elliptic curves?

Research is ongoing to develop quantum-resistant elliptic curve schemes or alternatives, as current elliptic curve cryptography can be broken by quantum algorithms like Shor's algorithm.

Additional Resources

1. *“The Arithmetic of Elliptic Curves” by Joseph H. Silverman*
This foundational text offers a comprehensive introduction to the theory of elliptic curves from an arithmetic perspective. It covers the basic properties, group law, and applications to number theory, including rational points and torsion subgroups. Silverman’s clear exposition makes it a standard reference for graduate students and researchers alike.

2. *“Advanced Topics in the Arithmetic of Elliptic Curves” by Joseph H. Silverman*
As a sequel to his first book, Silverman delves into more complex topics such as modular forms, Galois representations, and the Birch and Swinnerton-Dyer conjecture. It is intended for readers already familiar with the basics of elliptic curves and looking to explore deeper arithmetic properties. The text combines rigorous proofs with motivating examples.

3. *“Elliptic Curves: Number Theory and Cryptography” by Lawrence C. Washington*
This book bridges the gap between pure mathematics and practical applications by emphasizing both the theoretical aspects of elliptic curves and their role in modern cryptography. It covers the algebraic structure of elliptic curves and explains algorithms used in cryptographic protocols. Suitable for advanced undergraduates and beginning graduate students.

4. *“Rational Points on Elliptic Curves” by Joseph H. Silverman and John Tate*
Designed as an accessible introduction, this book focuses on the study of rational points on elliptic curves over the rational numbers. It uses

elementary techniques and minimal prerequisites, making it ideal for newcomers to the subject. The text includes numerous exercises and examples to facilitate understanding.

5. *“Elliptic Curves” by Anthony W. Knapp*
Knapp’s book provides a thorough introduction to the theory of elliptic curves with an emphasis on complex analysis and modular forms. It covers the complex uniformization theorem and the connection between elliptic curves and modular functions. The book is well-suited for readers interested in the analytic and geometric aspects of elliptic curves.

6. *“Modular Forms and Fermat’s Last Theorem” edited by Gary Cornell, Joseph H. Silverman, and Glenn Stevens*
This collection of essays explores the interplay between elliptic curves, modular forms, and the proof of Fermat’s Last Theorem. It offers contributions from leading experts, providing historical context as well as technical insights. The book is valuable for those interested in the modern developments linking elliptic curves to number theory.

7. *“The Theory of Elliptic Curves” by Neal Koblitz*
Koblitz’s text is a classic introduction to elliptic curves, covering both algebraic and arithmetic aspects. It emphasizes applications to cryptography, making it one of the pioneering books in the area. The clear style and inclusion of computational examples make it accessible to a broad audience.

8. *“Elliptic Curves in Cryptography” by Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart*
This book focuses specifically on the application of elliptic curves in cryptographic systems. It covers the mathematical background necessary for understanding elliptic curve cryptography (ECC) and details various algorithms and protocols. Ideal for computer scientists and engineers interested in secure communications.

9. *“Introduction to Elliptic Curves and Modular Forms” by Neal Koblitz*
Koblitz introduces readers to the rich theory connecting elliptic curves with modular forms, a central theme in modern number theory. The book balances rigorous mathematics with accessible explanations, making it suitable for advanced undergraduates and graduate students. It also discusses applications to cryptography and the proof of Fermat’s Last Theorem.

Elliptic Curves

elliptic curves: *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.

elliptic curves: Rational Points on Elliptic Curves Joseph H. Silverman, John T. Tate, 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.

elliptic curves: *Elliptic Curves* 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.

elliptic curves: *Elliptic Curves* Susanne Schmitt, Horst G. Zimmer, 2003 The content is kept as elementary as possible, and therefore the book differs significantly from the numerous textbooks on elliptic curves nowadays available. The book is addressed to graduate students and researchers in both mathematics and computer science.--BOOK JACKET.

elliptic curves: Modern Cryptography and Elliptic Curves 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.

elliptic curves: 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: Elliptic Functions and Elliptic Curves Patrick Du Val, 1973-08-02 A comprehensive treatment of elliptic functions is linked by these notes to a study of their application to elliptic curves. This approach provides geometers with the opportunity to acquaint themselves with aspects of their subject virtually ignored by other texts. The exposition is clear and logically carries themes from earlier through to later topics. This enthusiastic work of scholarship is made complete with the inclusion of some interesting historical details and a very comprehensive bibliography.

elliptic curves: The Arithmetic of Elliptic Curves Joseph H. Silverman, 2013-03-09 The preface to a textbook frequently contains the author's justification for offering the public another book on the given subject. For our chosen topic, the arithmetic of elliptic curves, there is little need for such an apologia. Considering the vast amount of research currently being done in this area, the paucity of introductory texts is somewhat surprising. Parts of the theory are contained in various books of Lang (especially [La 3] and [La 5]); and there are books of Koblitz ([Kob]) and Robert ([Rob], now out of print) which concentrate mostly on the analytic and modular theory. In addition, survey articles have been written by Cassels ([Ca 7], really a short book) and Tate ([Ta 5J, which is beautifully written, but includes no proofs). Thus the author hopes that this volume will fill a real need, both for the serious student who wishes to learn the basic facts about the arithmetic of elliptic curves; and for the research mathematician who needs a reference source for those same basic

facts. Our approach is more algebraic than that taken in, say, [La 3] or [La 5], where many of the basic theorems are derived using complex analytic methods and the Lefschetz principle. For this reason, we have had to rely somewhat more on techniques from algebraic geometry. However, the geom etry of (smooth) curves, which is essentially all that we use, does not require a great deal of machinery.

elliptic curves: Rational Points on Elliptic Curves Joseph H. Silverman, John Tate, 2013-04-17 In 1961 the second author deliv1lred a series of lectures at Haverford Col lege on the subject of Rational Points on Cubic Curves. These lectures, intended for junior and senior mathematics majors, were recorded, tran scribed, and printed in mimeograph form. Since that time they have been widely distributed as photocopies of ever decreasing legibility, and por tions have appeared in various textbooks (Husemoller [1], Chahal [1]), but they have never appeared in their entirety. In view of the recent inter est in the theory of elliptic curves for subjects ranging from cryptogra phy (Lenstra [1], Koblitz [2]) to physics (Luck-Moussa-Waldschmidt [1]), as well as the tremendous purely mathematical activity in this area, it seems a propitious time to publish an expanded version of those original notes suitable for presentation to an advanced undergraduate audience. We have attempted to maintain much of the informality of the orig inal Haverford lectures. Our main goal in doing this has been to write a textbook in a technically difficult field which is readable by the average undergraduate mathematics major. We hope we have succeeded in this goal. The most obvious drawback to such an approach is that we have not been entirely rigorous in all of our proofs. In particular, much of the foundational material on elliptic curves presented in Chapter I is meant to explain and convince, rather than to rigorously prove.

elliptic curves: 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 best evidence so far for the Birch and Swinnerton-Dyer conjecture.

elliptic curves: Elliptic Curves S. Lang, 1978-11-01 It is possible to write endlessly on elliptic curves. (This is not a threat.) We deal here with diophantine problems, and we lay the foundations, especially for the theory of integral points. We review briefly the analytic theory of the Weierstrass function, and then deal with the arithmetic aspects of the addition formula, over complete fields and over number fields, giving rise to the theory of the height and its quadraticity. We apply this to integral points, covering the inequalities of diophantine approximation both on the multiplicative group and on the elliptic curve directly. Thus the book splits naturally in two parts. The first part deals with the ordinary arithmetic of the elliptic curve: The transcendental parametrization, the p-adic parametrization, points of finite order and the group of rational points, and the reduction of certain diophantine problems by the theory of heights to diophantine inequalities involving logarithms. The second part deals with the proofs of selected inequalities, at least strong enough to obtain the finiteness of integral points.

elliptic curves: Elliptic Curves in Cryptography Ian F. Blake, G. Seroussi, N. Smart, 1999-07-08 This book summarizes knowledge built up within Hewlett-Packard over a number of years, and explains the mathematics behind practical implementations of elliptic curve systems. Due to the advanced nature of the mathematics there is a high barrier to entry for individuals and companies to

this technology. Hence this book will be invaluable not only to mathematicians wanting to see how pure mathematics can be applied but also to engineers and computer scientists wishing (or needing) to actually implement such systems.

elliptic curves: Elliptic Curves Lawrence C. Washington, 2003-05-28 Elliptic curves have played an increasingly important role in number theory and related fields over the last several decades, most notably in areas such as cryptography, factorization, and the proof of Fermat's Last Theorem. However, most books on the subject assume a rather high level of mathematical sophistication, and few are truly accessible to

elliptic curves: *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.

elliptic curves: Elliptic Curves, Modular Forms, and Their L-functions Álvaro 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.

elliptic curves: *Elliptic Curves* A. Robert, 1973

elliptic curves: *Introduction to Elliptic Curves and Modular Forms* Neal I. Koblitz, 2012-12-06 This textbook covers the basic properties of elliptic curves and modular forms, with emphasis on certain connections with number theory. The ancient congruent number problem is the central motivating example for most of the book. My purpose is to make the subject accessible to those who find it hard to read more advanced or more algebraically oriented treatments. At the same time I want to introduce topics which are at the forefront of current research. Down-to-earth examples are given in the text and exercises, with the aim of making the material readable and interesting to

mathematicians in fields far removed from the subject of the book. With numerous exercises (and answers) included, the textbook is also intended for graduate students who have completed the standard first-year courses in real and complex analysis and algebra. Such students would learn applications of techniques from those courses. thereby solidifying their under standing of some basic tools used throughout mathematics. Graduate stu dents wanting to work in number theory or algebraic geometry would get a motivational, example-oriented introduction. In addition, advanced under graduates could use the book for independent study projects, senior theses, and seminar work.

elliptic curves: 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 application

elliptic curves: Elliptic Curves and Related Topics H. Kisilevsky, Maruti Ram Murty, 1994-01-01 This book represents the proceedings of a workshop on elliptic curves held in St. Adele, Quebec, in February 1992. Containing both expository and research articles on the theory of elliptic curves, this collection covers a range of topics, from Langlands's theory to the algebraic geometry of elliptic curves, from Iwasawa theory to computational aspects of elliptic curves. This book is especially significant in that it covers topics comprising the main ingredients in Andrew Wiles's recent result on Fermat's Last Theorem.

elliptic curves: *The Arithmetic of Elliptic Curves* Joseph H. Silverman, 2009-05-29 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.

Related to elliptic curves

Elliptic curve - Wikipedia In mathematics, an elliptic curve is a smooth, projective, algebraic curve of genus one, on which there is a specified point O. An elliptic curve is defined over a field K and describes points in

An Introduction to the Theory of Elliptic Curves If E is an elliptic curve, then any function f (x; y) that does not vanish identically on E will have zeros and poles, each of which may occur with multiplicity one or larger

Elliptic Curves | Brilliant Math & Science Wiki Elliptic curves are curves defined by a certain type of cubic equation in two variables. The set of rational solutions to this equation has an extremely interesting structure, including a group law.

18.783 Elliptic Curves Lecture 1 - MIT Mathematics The elliptic curve factorization method (ECM), due to Lenstra, is a randomized algorithm that attempts to factor an integer n using random elliptic curves E=Q with a known point P 2 E(Q) of

Elliptic Curve -- from Wolfram MathWorld 3 days ago Informally, an elliptic curve is a type of cubic curve whose solutions are confined to a region of space that is topologically equivalent to a torus. The Weierstrass elliptic function

Elliptic Curves - Purdue University There is an elliptic curve variation of the Di e-Hellman key exchange algorithm in which the group Rp is replaced by an elliptic curve. In it, Alice and Bob agree on an elliptic curve E = Ea;b

Elliptic Curves: An Introduction - Columbia University The goal of the following paper will be

to explain some of the history of and motivation for elliptic curves, to provide examples and applications of the same, and to prove and discuss the

Elliptic curve - Wikipedia In mathematics, an elliptic curve is a smooth, projective, algebraic curve of genus one, on which there is a specified point O. An elliptic curve is defined over a field K and describes points in

An Introduction to the Theory of Elliptic Curves If E is an elliptic curve, then any function f (x; y) that does not vanish identically on E will have zeros and poles, each of which may occur with multiplicity one or larger

Elliptic Curves | Brilliant Math & Science Wiki Elliptic curves are curves defined by a certain type of cubic equation in two variables. The set of rational solutions to this equation has an extremely interesting structure, including a group law.

18.783 Elliptic Curves Lecture 1 - MIT Mathematics The elliptic curve factorization method (ECM), due to Lenstra, is a randomized algorithm that attempts to factor an integer n using random elliptic curves E=Q with a known point P 2 E(Q)

Elliptic Curve -- from Wolfram MathWorld 3 days ago Informally, an elliptic curve is a type of cubic curve whose solutions are confined to a region of space that is topologically equivalent to a torus. The Weierstrass elliptic function

Elliptic Curves - Purdue University There is an elliptic curve variation of the Di e-Hellman key exchange algorithm in which the group Rp is replaced by an elliptic curve. In it, Alice and Bob agree on an elliptic curve E = Ea;b

Elliptic Curves: An Introduction - Columbia University The goal of the following paper will be to explain some of the history of and motivation for elliptic curves, to provide examples and applications of the same, and to prove and discuss the

Elliptic curve - Wikipedia In mathematics, an elliptic curve is a smooth, projective, algebraic curve of genus one, on which there is a specified point O. An elliptic curve is defined over a field K and describes points in

An Introduction to the Theory of Elliptic Curves If E is an elliptic curve, then any function f (x; y) that does not vanish identically on E will have zeros and poles, each of which may occur with multiplicity one or larger

Elliptic Curves | Brilliant Math & Science Wiki Elliptic curves are curves defined by a certain type of cubic equation in two variables. The set of rational solutions to this equation has an extremely interesting structure, including a group law.

18.783 Elliptic Curves Lecture 1 - MIT Mathematics The elliptic curve factorization method (ECM), due to Lenstra, is a randomized algorithm that attempts to factor an integer n using random elliptic curves E=Q with a known point P 2 E(Q)

Elliptic Curve -- from Wolfram MathWorld 3 days ago Informally, an elliptic curve is a type of cubic curve whose solutions are confined to a region of space that is topologically equivalent to a torus. The Weierstrass elliptic function

Elliptic Curves - Purdue University There is an elliptic curve variation of the Di e-Hellman key exchange algorithm in which the group Rp is replaced by an elliptic curve. In it, Alice and Bob agree on an elliptic curve E = Ea;b

Elliptic Curves: An Introduction - Columbia University The goal of the following paper will be to explain some of the history of and motivation for elliptic curves, to provide examples and applications of the same, and to prove and discuss the

Related to elliptic curves

elliptic curve cryptography (PC Magazine6y) A public key cryptography method that provides fast decryption and digital signature processing. Elliptic curve cryptography (ECC) uses points on an elliptic curve to derive a 163-bit public key that

elliptic curve cryptography (PC Magazine6y) A public key cryptography method that provides fast decryption and digital signature processing. Elliptic curve cryptography (ECC) uses points on an

elliptic curve to derive a 163-bit public key that

Solana Co-Founder Says '50/50' Chance Quantum Computing Breaks Bitcoin By 2030, Calls For Quick Action (1d) The quantum computing threat to Bitcoin may be more urgent than some think, according to Solana co-founder Anatoly Yakovenko

Solana Co-Founder Says '50/50' Chance Quantum Computing Breaks Bitcoin By 2030, Calls For Quick Action (1d) The quantum computing threat to Bitcoin may be more urgent than some think, according to Solana co-founder Anatoly Yakovenko

Elliptic Curve Cryptography and Pairing Algorithms (Nature3mon) Elliptic curve cryptography (ECC) has emerged as a cornerstone of modern public-key systems, offering high levels of security with relatively small key sizes. Central to many advanced cryptographic

Elliptic Curve Cryptography and Pairing Algorithms (Nature3mon) Elliptic curve cryptography (ECC) has emerged as a cornerstone of modern public-key systems, offering high levels of security with relatively small key sizes. Central to many advanced cryptographic

Racing the quantum clock: ML-DSA faces real-world tests (14h) Post-quantum cryptography is here, and ML-DSA is leading the way. Experts from IBM and Qualcomm explain what's at stake for

Racing the quantum clock: ML-DSA faces real-world tests (14h) Post-quantum cryptography is here, and ML-DSA is leading the way. Experts from IBM and Qualcomm explain what's at stake for

Elliptic Curve Discrete Logarithm Problem (Nature3mon) The elliptic curve discrete logarithm problem (ECDLP) lies at the heart of modern public-key cryptography. It concerns the challenge of determining an unknown scalar multiplier given two points on an

Elliptic Curve Discrete Logarithm Problem (Nature3mon) The elliptic curve discrete logarithm problem (ECDLP) lies at the heart of modern public-key cryptography. It concerns the challenge of determining an unknown scalar multiplier given two points on an

ON ELLIPTIC CURVES WITH AN ISOGENY OF DEGREE 7 (JSTOR Daily11y) We show that if E is an elliptic curve over Q with a Q-rational isogeny of degree 7, then the image of the 7-adic Galois representation attached to E is as large as allowed by the isogeny, except for

ON ELLIPTIC CURVES WITH AN ISOGENY OF DEGREE 7 (JSTOR Daily11y) We show that if E is an elliptic curve over Q with a Q-rational isogeny of degree 7, then the image of the 7-adic Galois representation attached to E is as large as allowed by the isogeny, except for

Understanding Elliptic Curve Cryptography And Embedded Security (Hackaday6y) We all know the usual jokes about the 'S' in 'IoT' standing for 'Security'. It's hardly a secret that security in embedded, networked devices ('IoT devices') is all too often a last-minute task that

Understanding Elliptic Curve Cryptography And Embedded Security (Hackaday6y) We all know the usual jokes about the 'S' in 'IoT' standing for 'Security'. It's hardly a secret that security in embedded, networked devices ('IoT devices') is all too often a last-minute task that

ON THE RANK OF ELLIPTIC CURVES COMING FROM RATIONAL DIOPHANTINE TRIPLES (JSTOR Daily2mon) We construct a family of Diophantine triples $\{c_1(t), c_2(t), c_3(t)\}$ such that the elliptic curve over Q(t) induced by this triple, i.e.: $y^2 = (c_1(t)\,x + 1)(c_2(t)\,x + 1((c_3(t)\,x + 1)$ has torsion group

ON THE RANK OF ELLIPTIC CURVES COMING FROM RATIONAL DIOPHANTINE TRIPLES (JSTOR Daily2mon) We construct a family of Diophantine triples $\{c_1(t), c_2(t), c_3(t)\}$ such that the elliptic curve over Q(t) induced by this triple, i.e.: $y^2 = (c_1(t)\,x + 1)(c_2(t)\,x + 1((c_3(t)\,x + 1)$ has torsion group

Back to Home: http://www.speargroupllc.com