Access Free Introduction To Elliptic Curves And Modular Forms Graduate Texts In Mathematics No 97 Pdf Free Copy

Elliptic Curves Introduction to Elliptic Curves and Modular Forms **Elliptic Curves** Rational Points on Elliptic Curves **LMSST: 24 Lectures on Elliptic Curves Elliptic Curves Elliptic Curves Elliptic Curves Elliptic Curves Elliptic Curves (Second Edition) Algorithms for Modular Elliptic Curves Full Canadian Binding Elliptic Curves and Their Applications to Cryptography Elliptic Curves, Modular Forms, and Their L-functions Introduction to Elliptic Curves and Modular Forms** Elliptic Curves Advanced Topics in the Arithmetic of Elliptic Curves **Elliptic Curves Elliptic Curves, Hilbert Modular Forms and Galois Deformations** *Elliptic Curves and Arithmetic Invariants* The Arithmetic of Elliptic Curves *Elliptic Curves over Number Fields with Prescribed Reduction Type* **Elliptic Curves Guide to Elliptic Curve Cryptography** *Elliptic Curves in Cryptography* **Modern Cryptography and Elliptic Curves: A Beginner's Guide** *Arithmetic on Elliptic Curves with Complex Multiplication* **The Arithmetic of Elliptic Curves Elliptic Curve Public Key Cryptosystems Elliptic Curves Rational Points on Modular Elliptic Curves Arithmetic Moduli of Elliptic Curves. (AM-108), Volume 108** *Implementing Elliptic Curve Cryptography* **Arithmetic Theory of Elliptic Curves** *Rational Points on Elliptic Curves* **Discrete Mathematics and Its Applications** Elliptic Functions and Elliptic Curves One Semester of Elliptic Curves **Abelian l-Adic Representations and Elliptic Curves** *Geometric Modular Forms and Elliptic Curves* **Elliptic Tales**

If you ally craving such a referred **Introduction To Elliptic Curves And Modular Forms Graduate Texts In Mathematics No 97** book that will present you worth, acquire the utterly best seller from us currently from several preferred authors. If you want to hilarious books, lots of novels, tale, jokes, and more fictions collections are also launched, from best seller to one of the most current released.

You may not be perplexed to enjoy every books collections Introduction To Elliptic Curves And Modular Forms Graduate Texts In Mathematics No 97 that we will enormously offer. It is not a propos the costs. Its virtually what you craving currently. This Introduction To Elliptic Curves And Modular Forms Graduate Texts In Mathematics No 97, as one of the most keen sellers here will extremely be in the middle of the best options to review.

This is likewise one of the factors by obtaining the soft documents of this **Introduction To Elliptic Curves And Modular Forms Graduate Texts In Mathematics No 97** by online. You might not require more times to spend to go to the ebook initiation as capably as search for them. In some cases, you likewise pull off not discover the notice Introduction To Elliptic Curves And Modular Forms Graduate Texts In Mathematics No 97 that you are looking for. It will unquestionably squander the time.

However below, in imitation of you visit this web page, it will be suitably unconditionally simple to get as without difficulty as download guide Introduction To Elliptic Curves And Modular Forms Graduate Texts In Mathematics No 97

It will not say yes many time as we run by before. You can realize it even if accomplish something else at home and even in your workplace. fittingly easy! So, are you question? Just exercise just what we come up with the money for below as with ease as evaluation **Introduction To Elliptic Curves And Modular Forms Graduate Texts In Mathematics No 97** what you once to read!

When people should go to the book stores, search commencement by shop, shelf by shelf, it is really problematic. This is why we allow the books compilations in this website. It will unconditionally ease you to look guide **Introduction To Elliptic Curves And Modular Forms Graduate Texts In Mathematics No 97** as you such as.

By searching the title, publisher, or authors of guide you truly want, you can discover them rapidly. In the house, workplace, or perhaps in your method can be all best area within net connections. If you seek to download and install the Introduction To Elliptic Curves And Modular Forms Graduate Texts In Mathematics No 97, it is no question easy then, before currently we extend the associate to buy and create bargains to download and install Introduction To Elliptic Curves And Modular Forms Graduate Texts In Mathematics No 97 appropriately simple!

Eventually, you will unconditionally discover a extra experience and triumph by spending more cash. still when? realize you resign yourself to that you require to get those every needs subsequently having significantly cash? Why dont you attempt to get something basic in the beginning? Thats something that will lead you to comprehend even more on the globe, experience, some places, gone history, amusement, and a lot more?

It is your agreed own era to do something reviewing habit. accompanied by guides you could enjoy now is **Introduction To Elliptic Curves And Modular Forms Graduate Texts In Mathematics No 97** below.

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. 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. This book provides a comprehensive account of the theory of moduli spaces of elliptic curves (over integer rings) and its application to modular forms. The construction of Galois representations, which play a fundamental role in Wiles' proof of the Shimura?Taniyama conjecture, is given. In addition, the book presents an outline of the proof of diverse modularity results of two-dimensional Galois representations (including that of Wiles), as well as some of the author's new results in that direction.In this new second edition, a detailed description of Barsotti?Tate groups (including formal Lie groups) is added to Chapter 1. As an application, a down-to-earth description of formal deformation theory of elliptic curves is incorporated at the end of Chapter 2 (in order to make the proof of regularity of the moduli of elliptic curve more conceptual), and in Chapter 4, though limited to ordinary cases, newly incorporated are Ribet's theorem of full image of modular p-adic Galois representation and its generalization to ?big? ?-adic Galois representations under mild assumptions (a new result of the author). Though some of the striking developments described above is out of the scope of this introductory book, the author gives a taste of present day research in the area of Number Theory at the very end of the book (giving a good account of modularity theory of abelian ?-varieties and ?-curves). This classic book contains an introduction to systems of l-adic representations, a topic of great importance

in number theory and algebraic geometry, as reflected by the spectacular recent developments on the Taniyama-Weil conjecture and Fermat's Last Theorem. The initial chapters are devoted to the Abelian case (complex multiplication), where one 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. 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. A self-contained introductory text for beginning graduate students that is contemporary in approach without ignoring historical matters. 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. The theory of elliptic curves involves a pleasing blend of algebra, geometry, analysis, and number theory. This book 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 this book. 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. 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. After two decades of research and development, elliptic curve cryptography now has widespread exposure and acceptance. Industry, banking, and government standards are in place to facilitate extensive deployment of this efficient public-key mechanism. Anchored by a comprehensive treatment of the practical aspects of elliptic curve cryptography (ECC), this guide explains the basic mathematics, describes state-of-the-art implementation methods, and presents standardized protocols for public-key encryption, digital signatures, and key establishment. In addition, the book addresses some issues that arise in software and hardware implementation, as well as side-channel attacks and countermeasures. Readers receive the theoretical fundamentals as an underpinning for a wealth of practical and accessible knowledge about efficient application. Features & Benefits: * Breadth of coverage and unified, integrated approach to elliptic curve cryptosystems * Describes important industry and government protocols, such as the FIPS 186-2 standard from the U.S. National Institute for Standards and Technology * Provides full exposition on techniques for efficiently implementing finite-field and elliptic curve arithmetic * Distills complex mathematics and algorithms for easy understanding * Includes useful literature references, a list of algorithms, and appendices on sample parameters, ECC standards, and software tools This comprehensive, highly focused reference is a useful and indispensable resource for practitioners, professionals, or researchers in computer science, computer engineering, network design, and network data security. 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. 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 $\frac{22440351770433696992455751309066748631609484720418912332268928859588025535178967163570016480830}$. 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. 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. 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. Let K be an algebraic number field. The function attaching to each elliptic curve over K its conductor is constant on isoger. y classes of elliptic curves over K (for the definitions see chapter 1). ~Ioreover, for a given ideal a in OK the number of isogeny classes of elliptic curves over K with conductor a is finite. In these notes we deal with the following problem: How can one explicitly construct a set of representatives for the isogeny classes of elliptic curves over K with conductor a for a given ideal a in OK? The conductor of an elliptic curve over K is a numerical invariant which measures, in some sense, the badness of the reduction of the elliptic curve modulo the prime ideals in OK' It plays an important role in the famous Weil-Langlands conjecture on the connection between elliptic curves over K and congruence subgroups in 5L2(OK) * In case K ~ this connection can be stated as follows. For any ideal a = (N) in ~ let ro(N) be the congruence subgroup ro(N) { (: ~) E 5L2 (~) c E (N) } of 5L2 (~) and let 52 (fo (N» be the space of cusp forms of weight 2 for r 0 (N) Now Weil conjectured that there exists a bijection between the rational normalized eigenforms in 52(ro(N» for the Heckealgebra and the - 2 - Lsug~ny classes uf elliptic curves over ~ with conductor a = (N) . 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. These lecture notes grew out of a one semester introductory course on elliptic curves given to an audience of computer science and mathematics students, and assume only minimal background knowledge. After having covered basic analytic and algebraic aspects, putting special emphasis on explaining the interplay between algebraic and analytic formulas, they go on to some more specialized topics. These include the j-function from an algebraic and analytic perspective, a discussion of elliptic curves over finite fields, derivation of recursion formulas for the division polynomials, the algebraic structure of the torsion points of an elliptic curve, complex multiplication, and modular forms. In an effort to motivate basic problems the book starts very slowly but considers some aspects such as modular forms of higher level which are not usually treated. It presents more than 100 exercises and a Mathematica TM notebook that treats a number of calculations involving elliptic curves. The book is aimed at students of mathematics with a general interest in elliptic curves but also at students of computer science interested in their cryptographic aspects. The notes in this volume correspond to advanced courses held at the Centre de Recerca Matemàtica as part of the research program in Arithmetic Geometry in the 2009-2010 academic year. The notes by Laurent Berger provide an introduction to p-adic Galois representations and Fontaine rings, which are especially useful for describing many local deformation rings at p that arise naturally in Galois deformation theory. The notes by Gebhard Böckle offer a comprehensive course on Galois deformation theory, starting from the foundational results of Mazur and discussing in detail the theory of pseudo-representations and their deformations, local deformations at places l ? p and local deformations at p which are flat. In the last section,the results of Böckle and Kisin on presentations of global deformation rings over local ones are discussed. The notes by Mladen Dimitrov present the basics of the arithmetic theory of Hilbert modular forms and varieties, with an emphasis on the study of the images of the attached Galois representations, on modularity lifting theorems over totally real number fields, and on the cohomology of Hilbert modular varieties with integral coefficients. The notes by Lassina Dembélé and John Voight describe methods for performing explicit computations in spaces of Hilbert modular forms. These methods depend on the Jacquet-Langlands correspondence and on computations in spaces of quaternionic modular forms, both for the case of definite and indefinite quaternion algebras. Several examples are given, and applications to modularity of Galois representations are discussed. The notes by Tim Dokchitser describe the proof, obtained by the author in a joint project with Vladimir Dokchitser, of the parity conjecture for elliptic curves over number fields under the assumption of finiteness of the Tate-Shafarevich group. The statement of the Birch and Swinnerton-Dyer conjecture is included, as well as a detailed study of local and global root numbers of elliptic curves and their classification. The subject of elliptic curves is one of the jewels of nineteenth-century mathematics, originated by Abel, Gauss, Jacobi, and Legendre. This 1997 book presents an introductory account of the subject in the style of the original discoverers, with references to and comments about more recent and modern developments. It combines three of the fundamental themes of mathematics: complex function theory, geometry, and arithmetic. After an informal preparatory chapter, the book follows an historical path, beginning with the work of Abel and Gauss on elliptic integrals and elliptic functions. This is followed by chapters on theta functions, modular groups and modular functions, the quintic, the imaginary quadratic field, and on elliptic curves. Requiring only a first acquaintance with complex function theory, this book is an ideal introduction to the subject for graduate students and researchers in mathematics and physics, with many exercises with hints scattered throughout the text. This book contains a detailed account of the result of the author's recent Annals paper and JAMS paper on arithmetic invariant, including ?-invariant, L-invariant, and similar topics. This book can be regarded as an introductory text to the author's previous book p-Adic Automorphic Forms on Shimura Varieties. Written as a down-to-earth introduction to Shimura varieties, this text includes many examples and applications of the theory that provide motivation for the reader. Since it is limited to modular curves and the corresponding Shimura varieties, this book is not only a great resource for experts in the field, but it is also accessible to advanced graduate students studying number theory. Key topics include non-triviality of arithmetic invariants and special values of L-functions; elliptic curves over complex and p-adic fields; Hecke algebras; scheme theory; elliptic and modular curves over rings; and Shimura curves. This work is a comprehensive treatment of recent developments in the study of elliptic curves and their moduli spaces. The arithmetic study of the moduli spaces began with Jacobi's "Fundamenta Nova" in 1829, and the modern theory was erected by Eichler-Shimura, Igusa, and Deligne-Rapoport. In the past decade mathematicians have made further substantial progress in the field. This book gives a complete account of that progress, including not only the work of the authors, but also that of Deligne and Drinfeld. This volume contains the expanded versions of the lectures given by the authors at the C.I.M.E. instructional conference held in Cetraro, Italy, from July 12 to 19, 1997. The papers collected here are broad surveys of the current research in the arithmetic of elliptic curves, and also contain several new results which cannot be found elsewhere in the literature. Owing to clarity and elegance of exposition, and to the background material explicitly included in the text or quoted in the references, the volume is well suited to research students as well as to senior mathematicians. 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. Implementing Elliptic Curve Cryptography proceeds step-by- step to explain basic number theory, polynomial mathematics, normal basis mathematics and elliptic curve mathematics. With these in place, applications to cryptography are introduced. The book is filled with C code to illustrate how mathematics is put into a computer, and the last several chapters show how to implement several cryptographic protocols. The most important is a description of P1363, an IEEE draft standard for public key cryptography. The main purpose of Implementing Elliptic Curve Cryptography is to help "crypto engineers" implement functioning, state-of-the- art cryptographic algorithms in the minimum time. The basics of the theory of elliptic curves should be known to everybody, be he (or she) a mathematician or a computer scientist. Especially everybody concerned with cryptography should know the elements of this theory. The purpose of the present textbook is to give an elementary introduction to elliptic curves. Since this branch of number theory is particularly accessible to computer-assisted calculations, the authors make use of it by approaching the theory under a computational point of view. Specifically, the computer-algebra package SIMATH can be applied on several occasions. However, the book can be read also by those not interested in any computations. Of course, the theory of elliptic curves is

very comprehensive and becomes correspondingly sophisticated. That is why the authors made a choice of the topics treated. Topics covered include the determination of torsion groups, computations regarding the Mordell-Weil group, height calculations, S-integral points. The contents is kept as elementary as possible. In this way it becomes obvious in which respect the book differs from the numerous textbooks on elliptic curves nowadays available. This book presents an extensive set of tables giving information about elliptic curves. 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. 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. 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. 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. 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. 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 have been intensively studied in algebraic geometry and number theory. In recent years they have been used in devising efficient algorithms for factoring integers and primality proving, and in the construction of public key cryptosystems. Elliptic Curve Public Key Cryptosystems provides an up-to-date and self-contained treatment of elliptic curve-based public key cryptology. Elliptic curve cryptosystems potentially provide equivalent security to the existing public key schemes, but with shorter key lengths. Having short key lengths means smaller bandwidth and memory requirements and can be a crucial factor in some applications, for example the design of smart card systems. The book examines various issues which arise in the secure and efficient implementation of elliptic curve systems. Elliptic Curve Public Key Cryptosystems is a valuable reference resource for researchers in academia, government and industry who are concerned with issues of data security. Because of the comprehensive treatment, the book is also suitable for use as a text for advanced courses on the subject. These notes constitute a lucid introduction to ``Elliptic Curves", one of the central and vigorous areas of current mathematical research. The subject has been studied from diverse viewpoints--analytic, algebraic, and arithmetical. These notes offer the reader glimpses of all three aspects and present some of the basic important theorems in all of them. The first part introduces a little of the theory of Riemann surfaces and goes on to the study of tori and their projective embeddings as cubics. This part ends with a discussion of the identification of the moduli space of complex tori with the quotient of the upper half plane by the modular groups. The second part handles the algebraic geometry of elliptic curves. It begins with a rapid introduction to some basic algebraic geometry and then focuses on elliptic curves. The Rieman-Roch theorem and the Riemann hypothesis for elliptic curves are proved, and the structure of the endomorphism ring of an elliptic curve is described. The third and last part is on the arithmetic of elliptic curves over Q. The Mordell-Weil theorem, Mazur's theorem on torsion in rational points of an elliptic curve over Q, and theorems of Thue and Siegel are among the results which are presented. There is a brief discussion of theta functions, Eisenstein series and cusp forms with an application to representation of natural numbers as sums of squares. The notes end with the formulation of the Birch and Swinnerton-Dyer conjectures. There is an additional brief chapter (Appendix C), written in July 2004 by Kirti Joshi, describing some developments since the original notes were written up in the present form in 1992. 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. The companion Web site -- To the student -- The foundations : logic, sets, and functions -- The fundamentals : algorithms, the integers, and matrices -- Mathematical reasoning -- Counting -- Advanced counting techniques -- Relations -- Graphs -- Trees -- Boolean algebra -- Modeling computation