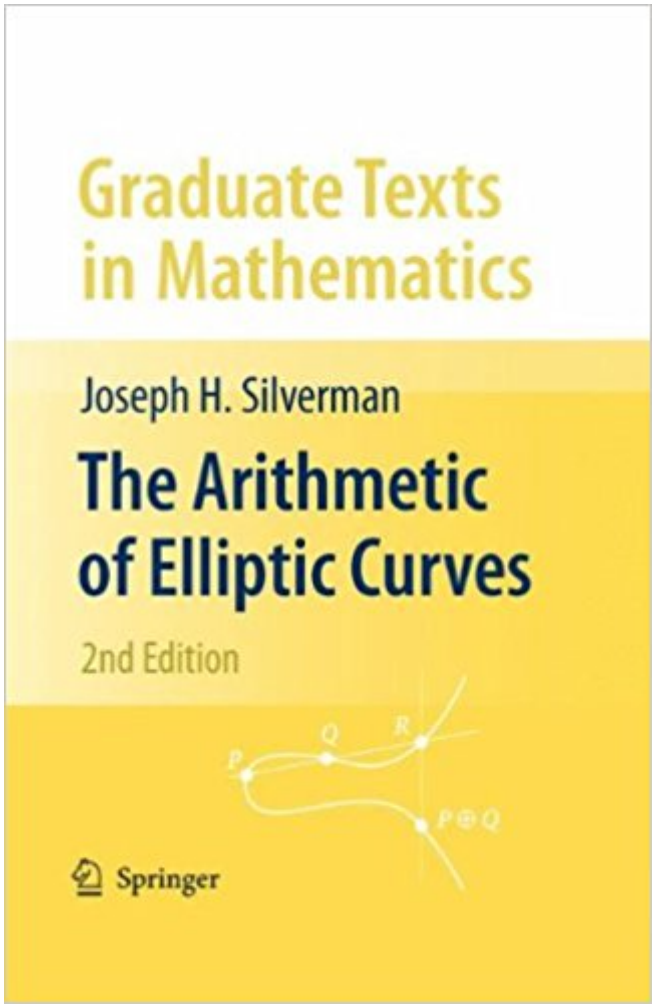
# The Arithmetic Of Elliptic Curves (Graduate Texts In Mathematics)



## Synopsis

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.

## Book Information

Series: Graduate Texts in Mathematics (Book 106)

Hardcover: 513 pages

Publisher: Springer; 2nd ed. 2009 edition (March 25, 2016)

Language: English

ISBN-10: 0387094938

ISBN-13: 978-0387094939

Product Dimensions: 6.1 x 1.2 x 9.2 inches

Shipping Weight: 1.9 pounds (View shipping rates and policies)

Average Customer Review: 5.0 out of 5 stars 4 customer reviews

Best Sellers Rank: #551,720 in Books (See Top 100 in Books) #77 inÃ Â Books > Science & Math > Mathematics > Geometry & Topology > Algebraic Geometry #177 inÃ Â Books > Science & Math > Mathematics > Pure Mathematics > Number Theory #315 inÃ Â Books > Textbooks > Science & Mathematics > Mathematics > Geometry

## Customer Reviews

From the reviews of the second edition:"This well-written book covers the basic facts about the geometry and arithmetic of elliptic curves, and is sure to become the standard reference in the subject. It meets the needs of at least three groups of people: students interested in doing research in Diophantine geometry, mathematicians needing a reference for standard facts about elliptic curves, and computer scientists interested in algorithms and needing an introduction to elliptic curves..."-- MATHEMATICAL REVIEWSÃ¢â ¬Å“The book under review is the second, revised, enlarged, and updated edition of J. SilvermanÃ¢â ¬â„¢s meanwhile classical primer of the

arithmetic of elliptic curves. Ã¢â ¬Â¦ All together, this enlarged and updated version of J. SilvermanÃ¢â ¬â„¢s classic Ã¢â ¬ËœThe Arithmetic of Elliptic CurvesÃ¢â ¬â„¢ significantly increases the unchallenged value of this modern primer as a standard textbook in the field. Ã¢â ¬Â¦ This makes the entire text a perfect source for teachers and students, for courses and self-study, and for further studies in the arithmetic of elliptic curves likewise.Ã¢â ¬Â• (Werner Kleinert, Zentralblatt MATH, Vol. 1194, 2010)Ã¢â ¬Å“For the second edition of his masterly book, the author considerably updated and improved several results and proofs. Ã¢â ¬Â¦ book contains a great many exercises, many of which develop or complement the results from the main body of the book. Ã¢â ¬Â¦ The reference list contains 317 items and reflects both classical and recent achievements on the topic. Notes on the exercises are an aid to the reader. Ã¢â ¬Â¦ Summarizing, this is an excellent book Ã¢â ¬Â¦ . useful both for experienced mathematicians and for graduate students.Ã¢â ¬Â•Ã Â- Ã Â- Ã Â- (Vasil' I. AndriÃ„Â- chuk, Mathematical Reviews, Issue 2010 i)Ã¢â ¬Å“This is the second edition of an excellent textbook on the arithmetical theory of elliptic curves Ã¢â ¬Â¦ . Although there are now a number of good books on this topic it has stood the test of time and become a popular introductory text and a standard reference. Ã¢â ¬Â¦ The author has added remarks which point out their significance and connection to those parts of the theory he presents. These will give readers a good start if they want to study one of them.Ã¢â ¬Â• (Ch. Baxa, Monatshefte fÃƒÂ r Mathematik, Vol. 164 (3), November, 2011)Ã¢â ¬Å“The book is written for graduate students Ã¢â ¬Â¦ and for researchers interested in standard facts about elliptic curves. Ã¢â ¬Â¦ A wonderful textbook on the arithmetic theory of elliptic curves and it is a very popular introduction to the subject. Ã¢â ¬Â¦ I recommend this book for anyone interested in the mathematical study of elliptic curves. It is an excellent introduction, elegant and very well written. It is one of the best textbooks to graduate level studies I have ever had contact yet.Ã¢â ¬Â• (Book Inspections Blog, 2012)

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 theory of elliptic curves in its modern formulation, through the use of basic algebraic number theory and algebraic geometry. The book begins with a brief discussion of the necessary algebro-geometric results, and proceeds with an exposition of the geometry of elliptic curves, the formal group of an elliptic curve, and elliptic curves over finite fields, the complex numbers, local fields, and global fields. Included are proofs of the MordellÃ¢â ¬â œWeil theorem giving finite generation of the group of rational points and Siegel's theorem on finiteness of integral points.  For this second edition of The Arithmetic of Elliptic

Curves, there is a new chapter entitled Algorithmic Aspects of Elliptic Curves, with an emphasis on algorithms over finite fieldsÃ Â which have cryptographic applications. These include Lenstra's factorization algorithm, Schoof's point counting algorithm, Miller's algorithm to compute the Tate and Weil pairings, and a description of aspects of elliptic curve cryptography. There is also a new section on Szpiro's conjecture and ABC, as well as expanded and updated accounts of recent developments and numerous new exercises. The book contains three appendices: Elliptic Curves in Characteristics 2 and 3, Group Cohomology, and a third appendix giving an overview of more advanced topics.

The theory of elliptic curves has to rank as one of the most fascinating fields in all of mathematics. Being around for almost two centuries, elliptic curves are finding myriads of applications, including cryptography, superstring theory, and computer imaging. The author does a brilliant job of organizing and explaining the theory in this book. Although the book requires a thorough understanding of algebraic geometry and modern algebra, the book is packed full of insights without sacrificing mathematical rigor. This is rare in most textbooks on modern mathematics. Numerous exercises exist at the end of each chapter, which allow readers to test their understanding of the subject as well as giving extensions to the main results in the text. The author reserves the cases of elliptic curves in characteristics 2 and 3 to the appendix. This may be disappointing for those reading the book for cryptographic applications of elliptic curves, but it does prepare one for further reading on the subject. By far the best chapter in the book is Chapter 10 on computing the Mordell-Weil group as the author does a nice job of detailing the relevant constructions. This book is well worth the time and effort required to study, and could serve well in an actual class on the subject. The author does have a follow-up book called "Advanced Topics in the Theory of Elliptic Curves" for those who need further stimulation in this intriguing and important field of mathematics.Addendum to review, Dec 12, 2009:The second edition of this book respects the same quality as the first.The new chapter on the algorithmic aspects of elliptic curves reflects the importance of elliptic curve cryptography since the appearance of the first edition and can be viewed as a warm-up for the study of cryptography over general Abelian varieties and for a study of group schemes. The author mentions group schemes when he discusses Lenstra's algorithm for elliptic curve factorization: the need for elliptic curves over rings Z/NZ when N is composite, and in the case of the elliptic curve discrete logarithm problem where there is a need for an "elliptic scheme", i.e. an elliptic curve over Z/p^2Z, where p is prime and greater than or equal to 3. The reader will get a taste of one of the algorithms for computing the Weil pairing and its generalization the

Tate-Lichtenbaum pairing. By some specialists in cryptography, the latter is considered to be a pairing that makes up for the deficiencies in the Weil pairing, namely that the Weil pairing is skew-symmetric. The author proves the nondegeneracy of the Tate-Litchtenbaum pairing in this chapter. Both the Weyl and Tate-Litchtenbaum pairings can be viewed in the more abstract, general framework of arithmetic duality theory and arithmetic geometry if one is willing to learn the appropriate techniques from Galois cohomology. In this framework the Tate-Litchtenbaum pairing for a (principally polarized) Abelian variety relates its Mordell-Weil group, its first cohomology group, and its Brauer group. For the author the value of the Tate-Litchtenbaum pairing over the Weil pairing is that the Miller algorithm for the Tate-Litchtenbaum pairing is twice as efficient as the Weil pairing. Included also in this chapter is a brief discussion of elliptic divisibility sequences (but delegated to the exercises), and references are given for their generalization in what are now called "elliptic nets", the latter of which is a recent development, and so it remains to be seen how much impact it will have on the computation of pairings.

Excellent book

This is a standard text now, and indeed it has it merits. The book uses algebraic geometry of curves throughout, instead of using the so-called ’Lefschetz principle’ as done in older texts like Serge Lang’s. Using general theorems of algebraic geometry instead of explicit polynomial calculation simplifies discussion, and at the same time paved the way for the reader towards the higher dimensional version of elliptic curves --- abelian varieties, whose geometry and arithmetic predate much of modern number theory research.After preliminary chapters on the underlying geometry of elliptic curves, the book take up its main aim -- proving the Mordell-Weil theorem, in chapter 8. The Mordell-Weil theorem states that the group of rational points over a number field is finitely generated, and finding the rank of this finitely generated abelian group effectively is subject to much current research (c.f. the Birch Swinnerton-dyer conjecture).The proof of Mordell-Weil theorem in this book is standard: one first establishes the weak version: E(F)/m E(F) for any integer m >1 , is a finite group. To prove this one has to know basic algebraic number theory, Kummer theory, and some Galois cohomology. For those who are not familiar with Galos cohomology, the author has provided an appendix on Galois cohomology, which should contain all that ’s needed.To deduce the full Mordell-Weil from the weak one, one establishes an important device: the theory of heights on elliptic curves. The height of a point is roughly a kind of norm, which measures the arithmetic complexity of the point (i.e. set of rational points with height bounded is finite) . The height function

come with a whole family, but there's a canonical one , the so-called Neron-Tate height, which actually is a quadratic form on the algebraic points of the elliptic curve. After establishing the property of this height, one nearly trivially deduce that the rational points must be finitely generated.The heights on elliptic curves and abelian varieties contain lots of (conjectured) information about the arithmetic of the varieties. One readily realise this when one look at the BSD conjecture, the Gross-Zagier formula, and various Diophantine approximation type conjecture (e.g. Vojta's) .Therefore it's worth spending time to study the theory of height. Unfortunately the author develop just that amount of theory to prove the Mordell-Weil theorem. For those who want furhter information , one can look at the book "Introduction to Diophantine Geometry" by M. Hindry and Silverman. But to really go to the heart of the matter, one must learn the intrinsic formulation of height by Arakelov (so-called Arakelov theory), as witnessed in Faltings' work on this subject.The Final two chapters are: Chapter 9 on integral points, Chapter 10 on computation of the weak Mordell-Weil group. Superficially, these 2 chapters are of completely different style: the theory of integral points employ classical Diophantine approximation technique, such as Roth's theorem and Baker's transcendence theory; while the theory of rational points (i.e. the structure of the Mordell-Weil group) employs the theoy of principal homogeneous space, Galois cohomology to measure failure of Hasse's principle, etc. As J. Tate had remarked in a 1974 article 'The theory of integral points on elliptic curves involves completely diffrent concepts (from rational points) and that we mention it only in passing...'. The situation now changed completely. The classical style of Diopahntine approximation, is employed by Vojta, Faltings, Bombieri to prove even stronger version of Mordell conjecture, which is about finitebess of rational points! The proof is much more elementary when compared to Falting's original proof. One can look at the book 'Diophantine approximation and abelian varieties' by Edihoxen and Everste for an introduction to this revival of the subject.But now back to this book written in 1986, the most importanr result of chapter 9 is Siegel 's theorem: finiteness of integral points on hyperelliptic curves, with application to the establishment of the Shafarevich conjecture of elliptic curves: finiteness of isomorphism class of elliptic curves with good reduction outside finite set of primes. (Note: the general Shafarevich conjecture lies at the heart of Faltings' original proof of the Mordell conjecture!). While Chapter 10 is an introduction to the Galois cohomology methos of calculating the weak Mordell -Weil group. Both theories and numerical examples are richly presented. In particular the important Selmer groups and Tate-Shafarevich group are introduced.Finding the 'size' of these two groups is subject to much current research. For example, bounding the size of a certain Selmer group lies at the heart of Wiles' proof of the semistable case of Shimura-Taniyama conjecture( hence Fermat). This is indeed

a very rich subject. For further information, one must studt further Galois chomology, arithmetic duality, Iwasawa theory, and finally Euler system.Overall, I think this book will appeal to anyone who want to know how to apply algebriac geometry to study Diophantine problems.

This is a superbly written introduction to elliptic curves. I like the straight-forward language. I dread the stiff elaborations, one finds in some german books with awkward idioms etc.. I found it fascinating, how the elements of general theory, explicit formulae and geometric ideas (the group law on an elliptic curve is constructed via means of geometry) are interwoven. However, if you want to get a glimpse of such fundamental theorems like the Mordell-Weil theorem, you will need a solid understanding of the basics of algebraic number theory. Also, if the author tells you "it is clear", it may take you two or three pages of your own thoughts and scribblings to actually see, why it is "clear". Sometimes it really is clear, but sometimes he might be referring to basic results from algebraic number theory. For example in VIII.$1 Proposition 1.6, a field is constructed, which is unramified outside a certain set of places of the number field K. The notion "It is clear .... is unramified if and only if ord_v(a) = 0 ..." had me puzzled for a while, until it dawned on me, that I needed a certain separability criterium for the polynomial to show what was needed. All in all, still a great book.

Characteristic Classes (Graduate Texts in Mathematics) Algebraic Geometry (Graduate Texts in Mathematics) Categories for the Working Mathematician (Graduate Texts in Mathematics) Algebraic Geometry: A First Course (Graduate Texts in Mathematics) (v. 133)