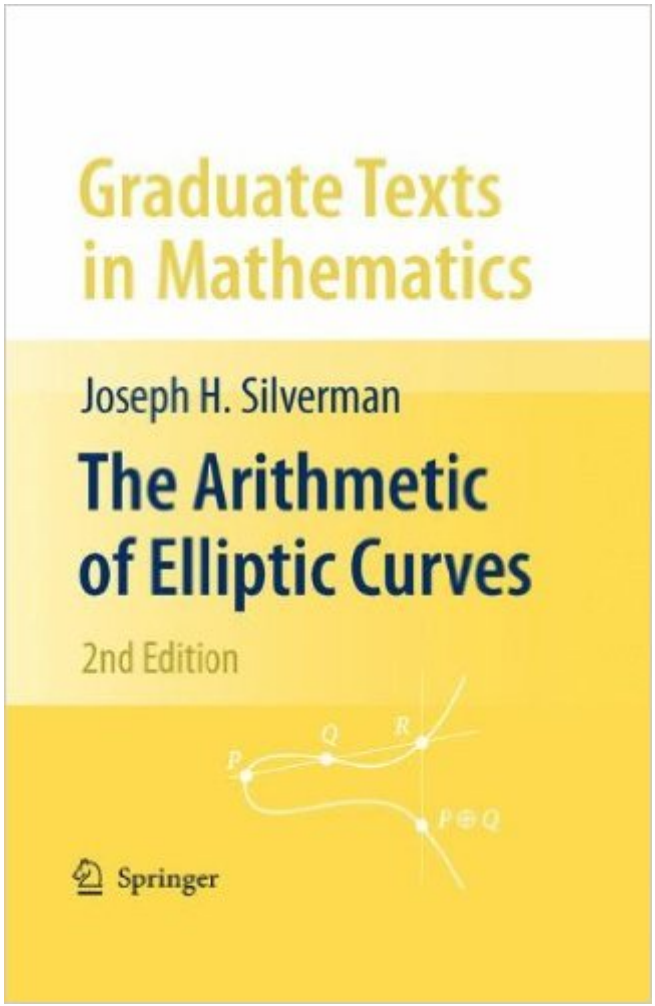
The Arithmetic Of Elliptic Curves (Graduate Texts In Mathematics)



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: 4.2 out of 5 starsÂ Â See all reviewsÂ (5 customer reviews)

Best Sellers Rank: #669,510 in Books (See Top 100 in Books) #83 inÂ Books > Science & Math > Mathematics > Geometry & Topology > Algebraic Geometry #224 inÂ Books > Science & Math > Mathematics > Pure Mathematics > Number Theory #384 inÂ Books > Textbooks > Science & Mathematics > Mathematics > Geometry

Customer Reviews

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 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.

(Undergraduate Texts in Mathematics) Elliptic Functions - An Elementary Text-Book for Students of Mathematics Arithmetic Geometry (Clay Mathematics Proceedings) Graph Theory (Graduate Texts in Mathematics) Functions of One Complex Variable II (Graduate Texts in Mathematics, Vol. 159) Algebraic Geometry (Graduate Texts in Mathematics) Categories for the Working Mathematician (Graduate Texts in Mathematics) Commutative Algebra: with a View Toward Algebraic Geometry (Graduate Texts in Mathematics) A First Course in Modular Forms (Graduate Texts in Mathematics) Rational Homotopy Theory (Graduate Texts in Mathematics) The Geometry of Schemes (Graduate Texts in Mathematics) Algebraic Geometry: A First Course (Graduate Texts in Mathematics) (v. 133) Introduction to Smooth Manifolds (Graduate Texts in Mathematics, Vol. 218) Introduction to Smooth Manifolds (Graduate Texts in Mathematics) Riemannian Manifolds: An Introduction to Curvature (Graduate Texts in Mathematics) Differential Geometry: Cartan's Generalization of Klein's Erlangen Program (Graduate Texts in Mathematics, Vol. 166)