Librería

Bonilla y Asociados

desde 1950

Título:

Autor:

Editorial:

Tema:

Precio: $768.00

Año: 2009

Edición: 2ª

ISBN: 9780387094939

Sinopsis

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 Mordell-Weil 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 fields 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.