

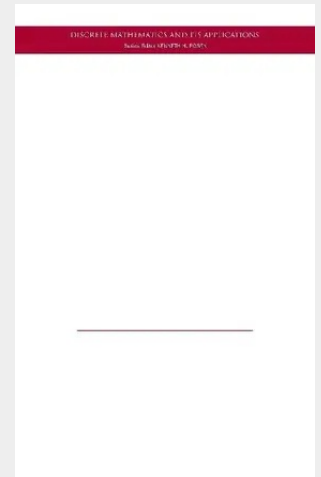
Washington

Elliptic Curves

Number Theory and Cryptography, Second Edition

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 $\mathbb{Q}$ - 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.

Like its bestselling predecessor, this second edition develops the theory of elliptic curves to provide a basis for both number theoretic and cryptographic applications. It now includes new chapters on isogenies and hyperelliptic curves, a more complete treatment of the Tate–Lichtenbaum pairing, alternative coordinate systems and related computational issues, and Doud's analytic method for computing torsion on elliptic curves over $\mathbb{Q}$. This edition also discusses how to perform computations with elliptic curves in several popular computer algebra systems. Basic exercises appear at the end of each chapter.



313,60 €

313,60 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9781420071467

Medium: Buch

ISBN: 978-1-4200-7146-7

Verlag: Chapman and Hall/CRC

Erscheinungstermin: 03.04.2008

Sprache(n): Englisch

Auflage: 2. Auflage 2008

Serie: Discrete Mathematics and Its Applications

Produktform: Gebunden

Gewicht: 1140 g

Seiten: 532

Format (B x H): 161 x 240 mm

