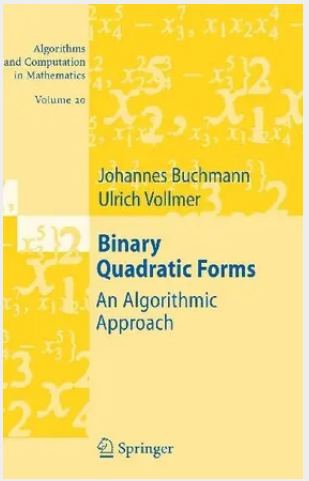
Buchmann / Vollmer

Binary Quadratic Forms

An Algorithmic Approach



The book deals with algorithmic problems related to binary quadratic forms. Written by a world leader in number theory, it is the only book focusing on the algorithmic aspects of the theory. It deals with problems such as finding the representations of an integer by a form with integer coefficients, finding the minimum of a form with real coefficients and deciding equivalence of two forms. In order to solve those problems, the book introduces the reader to important areas of number theory such as diophantine equations, reduction theory of quadratic forms, geometry of numbers and algebraic number theory. The book explains applications to cryptography. It requires only basic mathematical knowledge.

This book deals with algorithmic problems concerning binary quadratic forms 2 2 f(X,Y)= aX +bXY +cY with integer coe?cients a, b, c, the mathem- ical theories that permit the solution of these problems, and applications to cryptography. A considerable part of the theory is developed for forms with real coe?cients and it is shown that forms with integer coe?cients appear in a natural way. Much of the progress of number theory has been stimulated by the study of concrete computational problems. Deep theories were developed from the classic time of Euler and Gauss onwards to this day that made the solutions ofmanyof theseproblemspossible.Algorithmicsolutionsandtheirproperties became an object of study in their own right.
Thisbookintertwinestheexpositionofoneveryclassicalstrandofnumber theory with the presentation and analysis of algorithms both classical and modern which solve its motivating problems. This algorithmic approach will lead the reader, we hope, not only to an understanding of theory and solution methods, but also to an appreciation of the e? ciency with which solutions can be reached. The computer age has led to a marked advancement of algorithmic - search. On the one hand, computers make it feasible to solve very hard pr- lems such as the solution of Pell equations with large coe?cients. On the other, the application of number theory in public-key cryptography increased the urgency for establishing the complexity of several computational pr- lems: many a computer system stays only secure as long as these problems remain intractable.

53,49 €
49,99 € (zzgl. MwSt.)

Lieferfrist: bis zu 10 Tage

Artikelnummer: 9783540463672
Medium: Buch
ISBN: 978-3-540-46367-2
Verlag: Springer
Erscheinungstermin: 28.02.2007
Sprache(n): Englisch
Auflage: 1. Auflage 2007
Serie: Algorithms and Computation in Mathematics
Produktform: Gebunden
Gewicht: 670 g
Seiten: 318
Format (B x H): 160 x 241 mm