Review of the book

"Binary Quadratic Forms: An Algorithmic Approach"

by Johannes Buchmann & Ulrich Vollmer

Springer, 2007

ISBN: 978-3-540-46367-2

S.V.Nagaraj
RMK Engineering College

1 Summary of the review

Binary quadratic forms are quadratic forms in two variables. They have the form $ax^2+bxy+cy^2$. When a, b, and c are integers, the binary quadratic form is said to be integral. This book studies the theory of binary quadratic forms following an algorithmic approach. Applications of binary quadratic forms to cryptography are also described in the book which has twelve chapters and an appendix.

2 Summary of the book

The theory of quadratic forms has been well studied since the time of Euler and Gauss. This book revisits the theory of binary quadratic forms by taking an algorithmic approach. Important algorithms and some applications to cryptography are the highlight of this book which has twelve chapters and an appendix.

Chapter 1 (Binary Quadratic Forms)

This chapter introduces binary quadratic forms. The computational problems associated with them, the concept of discriminant, and applications of binary quadratic forms are described.

Chapter 2 (Equivalence of Forms)

This chapter presents the notion of equivalence of forms. Transformations of forms and their automorphisms are considered.

Chapter 3 (Constructing Forms)

This chapter studies the problem of constructing binary quadratic forms when the discriminant is given. The law of quadratic recciprocity, Kronecker symbols, and ways of computing square roots modulo primes are discussed here.

Chapter 4 (Forms, Bases, Points, and Lattices)

There are several ways of presenting the theory of quadratic forms. For example, points or lattices in a plane and continued fractions may be used for this purpose. This chapter looks at the correspondence between these representations.

Chapter 5 (Reduction of Positive Definite Forms)

This chapter focuses on the reduction theory of positive definite forms. It demonstrates that the reduction algorithm for such forms gives an efficient solution to the problem of deciding the equivalence between such forms.

Chapter 6 (Reduction of Indefinite Forms)

This chapter studies the reduction theory of indefinite forms. The results are different from that obtained for positive definite forms.

Chapter 7 (Multiplicative Lattices)

This chapter discusses the composition of forms by means of lattices. The notion of multiplicative lattices is introduced.

Chapter 8 (Quadratic Number Fields)

This chapter discusses the theory of quadratic number fields. Units of orders, ideals of orders, factorization of ideals, and unique factorization into prime ideals are studied.

Chapter 9 (Class Groups)

This chapter introduces the concept of class group. Ideals are used for this purpose Ambiguous ideals and classes, ways of computing in finite Abelian groups, and mechanisms for computing the structure of a finite Abelian group constitute the main focus of this chapter.

Chapter 10 (Infrastructure)

This chapter describes an algorithm known as the Terr algorithm which is useful in the context of real quadratic orders.

Chapter 11 (Sub-exponential Algorithms)

This chapter presents sub-exponential algorithms for class group and unit computation, and equivalence testing. The imaginary quadratic case and the real quadratic case are considered.

Chapter 12 (Cryptographic Applications)

This chapter studies the intractability of computational problems in quadratic fields. Examples of such problems include the discrete logarithm problem in the class group of imaginary quadratic orders and equivalence testing of ideals of real quadratic orders. Such problems may be used for cryptographic applications.

3 What is the book like (style)?

This book Binary Quadratic Forms - An Algorithmic Approach has been published as Volume 20 in the series "Algorithms and Computation in Mathematics" of Springer. The main author of the book Johannes Buchmann is a well-known computational number theory expert. The book consists of twelve chapters and an appendix. The appendix includes information about vectors, matrices, a lemma of Gauss, lattices, and linear algebra. The book explains the theory, algorithms, and applications of binary quadratic forms. The coverage is good and the description is exhaustive. The authors also try to focus on recent developments such as cryptographic applications of binary quadratic forms. Exercises have been

included at the end of chapters along with references and suggestions for further reading. This will be very useful for pedagogy and self-study. The authors have to be appreciated for considering an algorithmic approach to binary quadratic forms something which has not been done in books published earlier than this one. It is stated in the book that only basic mathematical knowledge is required. However, I wish to state that this is adequate for getting a feel of the subject, however, advanced concepts demand expertise in the subject.

4 Would you recommend this book?

The book will be useful for mathematicians especially number theorists, theoretical computer science specialists, students, faculty members and researchers in mathematics as well as computer science. I recommend this book as a useful reference and textbook on binary quadratic forms.

The reviewer is a professor of Computer Science and Engg. at RMK Engg. College, Kavaraipettai, India