ZMATH 2016f.01346

Diekert, Volker; Kufleitner, Manfred; Rosenberger, Gerhard; Hertrampf, Ulrich

Discrete algebraic methods. Arithmetic, cryptography, automata and groups.

De Gruyter Textbook. Berlin: De Gruyter (ISBN 978-3-11-041332-8/pbk; 978-3-11-041333-5/ebook). xii, 342 p. (2016).

A very successful attempt of creating a consise and "autonomous" presentation of discrete algebraic methods and its applications has been achieved through this book. It consists of eight chapters from which the first provides the algebraic structures needed as the foundations of the rest of the book. The next seven chapters define the applications of discrete algebraic methods as a future-oriented topic containing: cryptography, number theoretic algorithms, polynomial time primality test, elliptic curves, combinatorics on words, automata and discrete infinite groups. A remarquable achievement of the authors is that they do not just provide structured knowledged on the topic, but they pose questions and give specific answers. Should we use unproven security claims? Does it make sense to build cryptosystems on NP-hard problems? Why computations with elliptic curves are necessary? Moreover, areas of theoretical computer science are approached, for example at the chapter on automata or the algorithmic branch of combinatorial group theory at the final chapter. Mathematicians and computer scientists will surely enjoy the density of presentation of the various topics of the book. *Panayiotis Vlamos (Athena)*

Classification: P15 H45 F65
Keywords: cryptography; number theoretic algorithms; primality test; elliptic curves; automata; infinite groups
doi:10.1515/9783110413335