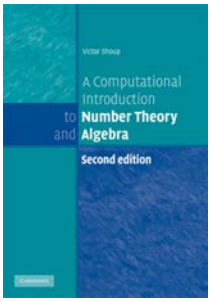
## Victor Shoup

## A Computational Introduction to Number Theory and Algebra[1]




Second edition, Cambridge University Press, Cambridge, 2009,

xviii+580 pp., ISBN 978-0-521-51644-0, £39,00

In recent decades, algebra and number theory have assumed an increasingly important role in communications and other fields of application. This is a surprising development, given that these fields of mathematics were once considered very pure and far away from the "real world". However, in order to connect the "pure" theory to its applications, one needs to develop it together with its computational aspects. This is what Victor Shoup's book does.

The book may be seen as a hybrid between two types of books which abound on the market: books on abstract algebra and number theory on the one hand, and books on computer algebra on the other. It is clear that such a hybrid book cannot be as comprehensive as any of the pure types. But including computational aspects and applications gives the theory a much richer context and thus provides a better motivation for readers. It also changes the flavor of the material: There is a difference between just learning that for an integer, there exists an inverse modulo some coprime integer, or learning how to compute this inverse by means of Euclid's algorithm.

The choice of material covered by the books seems to be guided by applications to cryptography (while coding theory plays a rather marginal role in the book). Therefore the focus of interest lies on integer arithmetic and on the arithmetic of the residue class rings of integers. Topics covered by the book that relate to integer arithmetic include the distribution of primes, probabilistic primality testing, and the recent deterministic primality testing algorithm by Agraval, Kayal, and Saxena. The latter, which is treated in the last chapter, is especially welcome, and certainly a culmination point of the book. Topics related to modular arithmetic include the discrete logarithm problem, quadratic reciprocity, and finite fields. Moreover, polynomial arithmetic and field extensions are treated in the book, and there are general chapters on abelian groups and commutative rings. So after having read this book, students will master a fair amount of abstract algebra.

The subject matter is presented in a very thorough way. For instance, the presentation of probabilistic algorithms is preceded by an introductory chapter on probability distributions. The book also devotes two sections to machine models and complexity theory. Detailed and clear proofs are given for (almost) all results. The material is very well organized: definitions, results, and their interrelations fit together perfectly. This thoroughness explains (and justifies) that the book is rather long (almost 600 pages) while it does not cover that much material.

The book assumes very little mathematical background in terms of knowledge, but it does assume some mathematical experience. The audience will consist mostly of graduate and upper-division undergraduate students in mathematics or computer science. The book is especially attractive to students with a background or interest in computer science. On the other hand, students who already have a background in abstract algebra can benefit greatly from this book by skipping some of the parts where algebraic theory is introduced. The use of the book as a textbook for graduate or undergraduate courses may be somewhat limited due to its length and due to its hybrid nature. But it is highly suitable for self study.

The suitability of the book for self-study is greatly enhanced by a wealth of exercises and examples that are provided. The focus of the examples and exercises lies on quantity rather than on difficulty. For example, Chapter 8 has 61 examples and 72 exercises. In my understanding of teaching mathematics, this is a strength: For getting a good grasp of the material, it helps students more to do a lot of exercises of moderate difficulty than to do a few very difficult ones. Last but not least, the book is very well-written, and it is a pleasure to read it.

*Gregor Kemper (München)*

Weitere Bücher können auf der Seite `http://www.fachgruppe-computeralgebra.de/Buecher` oder direkt bei Anne Frühbis-Krüger (`fruehbis-krueger@math.uni-hannover.de`) zur Besprechung angefordert werden.

[1]This review has originally appeared in *Mathematics of computation*, Volume 79, Number 270, April 2010, Pages 1231–1232, and is reprinted with kind permission of the American Mathematical Society.