MATHEMATICS OF COMPUTATION
Volume 76, Number 259, July 2007, Pages 1697–1698
S 0025-5718(07)01995-3
Article electronically published on February 5, 2007

5[11Txx, 11Yxx, 13Pxx, 68Qxx, 68Wxx]—*A computational introduction to number theory and algebra*, by Victor Shoup, Cambridge University Press, Cambridge, 2005, xvi + 517 pp., US$55.00, hardcover, ISBN 0-521-85154-8

It is well known that computational number theory and algebra are versitile areas with many applications to cryptography, coding theory, theoretic computer science, and a number of other areas. However, despite that the area has a clear orientation on applications, one should not treat these areas as merely convenient tools. Their problems and methods are of independent value and lead to a wealth of really beautiful and diverse mathematics.

On the other hand, there are very few self-contained expositions of this area which are suitable for beginners. The main purpose of this book is to fill this gap, and this purpose has been fully achieved.

The book is written by a real expert in the area, who has extensive first-hand experience in both theoretic and practical aspects of algorithm design and cryptography.

The underlying motif of the book is that after answering the question, "What is X?", it immediately proceeds to ask, "How can we compute X and how fast?".

In a systematic way, it introduces basic notions of elementary number theory and algebra, including divisibility and primality, congruences, prime number factorisation, the greatest common divisor, polynomials, matrices, groups and rings, and modular arithmetic, just to name a few. Then it proceeds with more advanced topics, some of which are right on edge of current research activities. For example, it presents primality testing algorithms, algorithms to construct irreducible polynomials, primitive roots and quadratic non-residues, subexponential integer factorisation and discrete logarithm algorithms, and many others. It also contains some necessary background material on probability theory and complexity theory. Cryptographic application can be found throughout the book as well.

The abundance of exercises and examples will keep the readers active, helping them to understand the material, clarify the most crucial ideas, and maybe even generate and try several new approaches.

It is also very important to note that the author has decided to keep this book "alive" and thus he maintains a website with an errata and lots of supplementary material. Moreover, the book itself is freely available from the same website (no, this is not a mistake, the book can indeed be downloaded from Victor Shoup's homepage). The author certainly deserves a standing ovation for arranging this free access with the publisher.

Certainly giving a full survey of the area has never been a purpose of this book. However, maybe providing a more complete bibliography list would be beneficial for the book. For example, Section 10.5 on perfect power testing would deliver a more complete picture if it contained a reference to the work of D. Bernstein. Probably one would also expect a reference to H. Cohen's books on computational algebraic number theory. Maybe also a short section about primality proofs would fit rather nicely into this book. Especially so, since the original deterministic primality test of M. Agrawal, N. Kayal and N. Saxena, which is deemed as impractical in the book, has found very important and practical applications to this problem. In passing, we also mention that it is a pity that [6] (that is, the AKS paper), has

not been updated to a reference to its journal version, which appeared in Annals of Mathematics, vol. 160, 2004, 781–793.

Despite the above minor critical comments, the book gives a very nice impression and is a real pleasure to read. Without doubt, it will be of great use for already active researchers as well as for beginners and can certainly be used for graduate courses on computational number theory.

Igor Shparlinski
E-mail address: igor@comp.mq.edu.au