Review of the book

"Elementary Number Theory, Cryptography and Codes"

by M.W. Baldoni, C. Ciliberto, and G.M. Piacentini Cattaneo

Springer, 2009

ISBN: 978-3-540-69199-0

Yeşem Kurt Peker
Randolph College

25 May 2010

1 Summary of the review

The book is an almost classical treatment of number theory and its applications to cryptography and coding theory. It involves more abstract notions than a classical elementary number theory book does and requires the reader to be familiar with certain algebraic structures. Even though it is written to contain all the necessary definitions, at some places the generalizations may be too abrupt for a reader who does not have a good understanding of abstraction. A prerequisite to fully benefit from this book would be a course in abstract algebra.

2 Summary of the book

The book has 9 chapters. The first five chapters, especially the earlier sections in each of them are devoted to explaining the theory on which the applications in the rest of the book build.

Chapter 1 starts with a list of topics that the reader should be familiar with. It goes on with fundamental topics such as mathematical induction, recursion, Fibonacci Numbers, Euclidean Algorithm, operations in different bases, and continued fractions.

Chapter 2 is devoted to one of the main components of cryptology, namely complexity theory. The chapter starts with the motivation behind complexity theory and continues on more rigorously to definitions of complexity, the Big-O notation, and polynomial and exponential time complexities. Then it discusses the complexity of basic operations followed by complexity of some essential algorithms in cryptography.

Chapter 3 is on another fundamental concept in number theory: congruences. Properties and applications of congruences, and the Chinese Remainder Theorem find their places in this chapter.

Chapter 4 starts with explaining the importance of prime numbers and the fundamental theorems involving prime numbers such as the Fundamental Theorem of Arithmetic, Euler's Theorem, and others. It continues with the problem of factoring integers and discusses some of the algorithms for factoring.
Chapter 5 introduces finite fields and states, with proofs, many theorems about finite fields that are heavily used in the later chapters. Quadratic residues and the Legendre symbol are also treated in this chapter.
Chapters 6 through 9 are mostly about applications of the theory. An essential topic in cryptography, primality, is discussed in Chapter 6 along with more methods for factoring integers.
Chapter 7 covers several aspects of cryptography starting with classical ciphers, continuing on to modern ciphers and public key cryptosystems, and cryptanalysis of some ciphers. Theory on elliptic and hyperelliptic curves and cryptosystems on these curves are also discussed in Chapter 7.
Chapter 8 discusses data transmission over a noisy channel, develops the necessary theory in information science and explains various codes including linear, cyclic, and Goppa codes.
Chapter 9 ventures into the quantum world and talks about quantum computers and the very basic theories of quantum mechanics as they apply to quantum cryptography.
At the end of each chapter, there is an appendix that contains the exercises for that chapter. Exercises are divided into three categories on three different aspects of the topics discussed; namely theoretical, computational, and programmable aspects.

3 What is the book like (style)?

The book is written as a textbook for a course in elementary number theory and its applications to cryptography and coding theory. It involves more abstract notions than a classical elementary number theory book does and requires the reader to be familiar with algebraic structures such as semigroups, groups, rings, integral domains, and fields. It is written in a scientific style and as such provides rigorous proofs of the theorems introduced. It covers a broad range of topics in number theory as they apply to cryptography and coding theory. The theory, applications, and algorithms are all illustrated with good examples worked out in detail. The exercises are divided into three categories (theoretical, computational, and programming exercises) and are placed at the end of each chapter. Some of the problems are multiple-choice which is a good idea as it may be less intimidating for a start for students. Hints and answers to many of the problems are provided at the end of the book.

4 Would you recommend this book?

Yes, I would recommend the book to various readers. The book speaks more to a mathematically mature reader who has a good understanding of abstraction. It is a well-written book in terms of the rigor, examples, and the exercises it includes. For undergraduate level students, a course in abstract algebra would be required to fully understand many of the topics included in the book.

The reviewer is a professor of mathematics at Randolph College, Lynchburg, VA.