Review of the book

"Primality Testing in Polynomial Time
From Randomized Algorithms to "PRIMES Is in P""

by Martin Dietzfelbinger

Springer, 2004

ISBN: 978-3-540-40344-9

Abderrahmane Nitaj
Laboratoire de Mathématiques Nicolas Oresme
Université de Caen Basse Normandie, France

January 4, 2012

1 Summary of the review

Primality testing is a fundamental tool in computational number theory and cryptography. Prime numbers have a long tradition in various modern cryptosystems. They are at the heart of RSA (Rivest, Shamir and Adleman, 1978), El Gamal (1985) and Diffie-Helleman (1976) and are expected to be extensively used in a variety of applications in the future.
There are various tests to determine whether a given number is prime. The most useful primality tests can be divided into two main classes, probabilistic or deterministic. The probabilistic class contains mainly Fermat primality test, Solovay-Strassen primality test and Miller-Rabin primality test, while deterministic class contains the Elliptic curve primality proving test and AKS primality test of M. Agrawal, N. Kayal, and N. Saxena.
The book is about the Primality Testing. It deeply describes all the former tests and analyzes their complexities as well as a variety of results from number theory, groups, rings, fields and polynomials. I particularly appreciated the chapter devoted to the deterministic primality test AKS.

2 Summary of the book

As the title says this book is about Primality Testing. It begins from the well known classical primality tests and covers the latest developments including the AKS test. This self contained book includes eight chapters and an appendix. It reviews the definitions of the basic concepts from number theory and algebra to a full understanding of the latest developments of primality tests.

- **Chapter 1: Introduction: Efficient Primality Testing**
  Chapter 1 contains a general introduction to the necessary basic on algorithms for Primality Testing which includes the notions of polynomial and superpolynomial time bounds and randomized and superpolynomial time algorithms for the Primality Problem.

- **Chapter 2: Algorithms for Numbers and Their Complexity**
  Chapter 2 is very short and contains standard notations for algorithms on numbers and complexities of some elementary operations with integers.

- **Chapter 3: Fundamentals from Number Theory**
  Chapter 3 covers the fundamental material on Number Theory including the Euclidean Algorithm, the Modular Arithmetic, the Chinese Remainder Theorem and a full of results on prime numbers.

- **Chapter 4: Basics from Algebra: Groups, Rings, and Fields**
  Chapter 4 covers the fundamental material on Groups, Rings, Fields and Finite Fields.

- **Chapter 5: The Miller-Rabin Test**
  Chapter 5 covers the Miller-Rabin test as well as the Fermat Test and Carmichael numbers. The algorithms are straightforwardly described and their complexities are analyzed.

- **Chapter 6: The Solovay-Strassen Test**
  Chapter 6 is focusing on the Solovay-Strassen test. It recovers the necessary tools to understand the test, namely the notions of quadratic residues, the Legendre and Jacobi symbols and the quadratic reciprocity law. The chapter ends with an analysis of the complexity of the Solovay-Strassen test.

- **Chapter 7: More Algebra: Polynomials and Fields**
  Chapter 7 covers basic topics on the theory of polynomials over rings and fields. It describes the arithmetical operations on polynomials, the division with remainder and divisibility as well as irreducible polynomials and factorization. The chapter is a preparation for the correctness proof of the deterministic primality test of Agrawal, Kayal, Saxena (AKS).

- **Chapter 8: Deterministic Primality Testing in Polynomial Time**
  Chapter 8 presents AKS, the deterministic primality-proving algorithm created and published by Agrawal, Kayal and Saxena in 2002. The chapter describes the basic idea and the algorithm of AKS. The running time is analyzed and the proof and the correctness of the algorithm is provided. The chapter begins with a characterization of prime numbers in terms of certain polynomial powers followed by a detailed description of the AKS test. The rest of the chapter is devoted to the correctness proof.

- **Appendix:**
  In the appendix, the author provides some useful results and number theoretical functions needed by the various primality tests. Typical examples are the factorial function and the binomial coefficients. The Appendix and the book terminate with a proof of the quadratic reciprocity law.

3 What is the book like (style)?

The text is written in a clear style, and the topics are described carefully. The numerous algorithms are clearly described and analyzed. Moreover, most of the number theoretical notions are illustrated by numerical examples. This makes the book enjoyable and very easy to follow.

4 Would you recommend this book?

This book provides a good starting point for Primality Testing, regardless of the background of the reader: computer science, mathematics, or any other discipline in which the use of prime numbers is required. I readily recommend this book to advanced undergraduates and the beginning graduate students interested in prime numbers, factorization and cryptographic systems based on large prime numbers.

The reviewer is a researcher with LMNO, Université de Caen Basse Normandie, France