Review of the book

"Prime Numbers and Computer Methods for Factorization"

Reprint of Second Edition published in 1994

by Hans Riesel

Birkhäuser

Springer 2012

ISBN: 978-0-8176-8297-2

S. V. Nagaraj

2015-04-01

1 Summary of the review

Cryptography is the science of secret codes. Modern cryptography is based heavily on number theory. One of the most famous cryptosystems is the RSA cryptosystem named after its inventors Rivest, Shamir and Adleman. The strength of this cryptosystem lies in the difficulty in factoring large integers. This review is about a book on prime numbers and computer methods for integer factorization. The book is a reprint of the second edition which was published by Birkhäuser in the year 1994. It has been published in the Modern Birkhäuser Classics series. This series includes specially chosen classics re-released (without any modifications) in both paperback and ebook formats. The book has seven chapters and eleven appendices.

2 Summary of the book

The book contains information about prime numbers and techniques for factorizing integers. It includes seven chapters and eleven appendices.

Chapter 1 (The Number of Primes Below a Given Limit) includes information about the sieve of Eratosthenes, tables of primes, and techniques for counting the number of primes below a given limit such as Meissel's formula, Lehmer's formula, and the Mapes' algorithm.

Chapter 2 (The Primes Viewed at Large) looks at formulae yielding primes, the distribution of primes, the prime number theorem, the Chebyshev function, the Riemann zeta function, zeroes of the zeta function, Riemann's prime number formula, inequalities, and the number of primes in arithmetic progressions.

Chapter 3 (Subtleties in the Distribution of Primes) studies the distribution of primes in short intervals, prime twins and other constellation of primes, the Hardy-Littlewood constants, the prime k-tuples conjecture, the midpoint sieve, dense clusters of primes, large gaps between consecutive primes, and conjectures related to primes.

Chapter 4 (The Recognition of Primes) describes tests of primality and compositeness, the use of Fermat's theorem for primality testing and compositeness testing, pseudoprimes and probable primes, Carmichael numbers, Euler pseudoprimes, strong pseudoprimes, other types of pseudoprimes, tests for primality such as the Adleman Pomerance Rumely Cohen Lenstra (APRCL) test, elliptic curve primality proving, the Goldwasser-Kilian test, and Atkin's test.

Chapter 5 (Classical Methods of Factorization) discusses trial division, factoring methods due to Fermat, Euler, Gauss, and Legendre, the Erdős-Kac theorem, smooth numbers, and the search for factors of certain forms.

Chapter 6 (Modern Factorization Methods) looks at Pollard's $p-1$ method, Pollard's rho method, methods due to Brent, Shanks and others, the quadratic sieve method, the multiple polynomial quadratic sieve, the Schnorr-Lenstra method, the elliptic curve method of Lenstra, the number field sieve and its generalization, and the complexity of factoring.

Chapter 7 (Prime Numbers and Cryptography) studies practical secrecy, keys used in cryptography, the RSA cryptosystem, and the safety of the RSA cryptosystem.

There are eleven appendices which include information about basic concepts in higher algebra, basic concepts in higher arithmetic, quadratic residues, the arithmetic of quadratic fields, higher algebraic number fields, algebraic factors, elliptic curves, continued factions, multiple–precision arithmetic, fast multiplication of large integers, and the Stieltjes integral.

There are 24 tables providing data on factors and miscellaneous details. There is a list of textbooks for further reading and a useful index.

3 What is the book like (style)?

The book offers a very good introduction to concepts related to prime numbers and computer methods for factoring integers. The original second edition published in 1994 is indeed a classic. The effort of the publisher Birkhäuser to reprint the classic unmodified in its Modern Classics Series is indeed appreciable. The paperback and ebook versions will be very useful for the current generation of students and researchers. Although it is over 20 years since the original second edition was published in 1994, the key ideas related to prime numbers and factorization methods are still unchanged. However, since 1994 many developments have taken place in the field of prime numbers as well as computer methods for factorization. For instance, many new results are known regarding primes such as the Agarwal Kayal Saxena deterministic polynomial time primality test. Computing power has grown significantly, consequently, for the safety of cryptosystems, the key size has gone up. Parallel processing and the Internet are helpful in factoring large numbers. The book is well written and highly readable, so it is ideal for beginners and undergrads. I feel a revised edition taking into account the developments since 1994 will be even more helpful.

4 Would you recommend this book?

This book is a reprint of a classic on primes and integer factorization methods. I strongly recommend this book as well as its ebook version for all enthusiasts of number theory and cryptography.

The reviewer is a freelancer in Chennai, India