

# 《Primality Testing in》

## 图书基本信息

书名：《Primality Testing in Polynomial Time多项式时间中的初级测试》

13位ISBN编号：9783540403449

10位ISBN编号：3540403442

出版社：Springer

作者：Dietzfelbinger, Martin

版权说明：本站所提供下载的PDF图书仅提供预览和简介以及在线试读，请支持正版图书。

更多资源请访问：[www.tushu000.com](http://www.tushu000.com)

# 《Primality Testing in》

## 内容概要

This book is devoted to algorithms for the venerable primality problem: Given a natural number  $n$ , decide whether it is prime or composite.

The problem is basic in number theory, efficient algorithms that solve it, i.e., algorithms that run in a number of computational steps which is polynomial in the number of digits needed to write  $n$ , are important for theoretical computer science and for applications in algorithmics and cryptology.

This book gives a self-contained account of theoretically and practically important efficient algorithms for the primality problem, covering the randomized algorithms by Solovay-Strassen and Miller-Rabin from the late 1970s as well as the recent deterministic algorithm of Agrawal, Kayal, and Saxena. The textbook is written for students of computer science, in particular for those with a special interest in cryptology, and students of mathematics, and it may be used as a supplement for courses or for self-study.

## 书籍目录

1. Introduction: Efficient Primality Testing
  - 1.1 Algorithms for the Primality Problem
  - 1.2 Polynomial and Superpolynomial Time Bounds
  - 1.3 Is PRIMES in P?
  - 1.4 Randomized and Superpolynomial Time Algorithms for the Primality Problem
  - 1.5 The New Algorithm
  - 1.6 Finding Primes and Factoring Integers
  - 1.7 How to Read This Book
2. Algorithms for Numbers and Their Complexity
  - 2.1 Notation for Algorithms on Numbers
  - 2.2 O-notation
  - 2.3 Complexity of Basic Operations on Numbers
3. Fundamentals from Number Theory
  - 3.1 Divisibility and Greatest Common Divisor
  - 3.2 The Euclidean Algorithm
  - 3.3 Modular Arithmetic
  - 3.4 The Chinese Remainder Theorem
  - 3.5 Prime Numbers
    - 3.5.1 Basic Observations and the Sieve of Eratosthenes
    - 3.5.2 The Fundamental Theorem of Arithmetic
  - 3.6 Chebychev's Theorem on the Density of Prime Numbers
4. Basics from Algebra: Groups, Rings, and Fields
  - 4.1 Groups and Subgroups
  - 4.2 Cyclic Groups
    - 4.2.1 Definitions, Examples, and Basic Facts
    - 4.2.2 Structure of Cyclic Groups
    - 4.2.3 Subgroups of Cyclic Groups
  - 4.3 Rings and Fields
  - 4.4 Generators in Finite Fields
5. The Miller-Rabin Test
  - 5.1 The Fermat Test
  - 5.2 Nontrivial Square Roots of 1
  - 5.3 Error Bound for the Miller-Rabin Test
6. The Solovay-Strassen Test
  - 6.1 Quadratic Residues
  - 6.2 The Jacobi Symbol
  - 6.3 The Law of Quadratic Reciprocity
  - 6.4 Primality Testing by Quadratic Residues
7. More Algebra: Polynomials and Fields
  - 7.1 Polynomials over Rings
  - 7.2 Division with Remainder and Divisibility for Polynomials...
  - 7.3 Quotients of Rings of Polynomials
  - 7.4 Irreducible Polynomials and Factorization
  - 7.5 Roots of Polynomials
  - 7.6 Roots of the Polynomial  $X^r - 1$
8. Deterministic Primality Testing in Polynomial Time
  - 8.1 The Basic Idea

# 《Primality Testing in》

- 8.2 The Algorithm of Agrawal, Kayal, and Saxena
- 8.3 The Running Time
  - 8.3.1 Overall Analysis
  - 8.3.2 Bound for the Smallest Witness  $r$
  - 8.3.3 Improvements of the Complexity Bound
- 8.4 The Main Theorem and the Correctness Proof
- 8.5 Proof of the Main Theorem
  - 8.5.1 Preliminary Observations
  - 8.5.2 Powers of Products of Linear Terms
  - 8.5.3 A Field  $F$  and a Large Subgroup  $G$  of  $F^*$  .
  - 8.5.4 Completing the Proof of the Main Theorem

## A. Appendix

- A.1 Basics from Combinatorics
- A.2 Some Estimates
- A.3 Proof of the Quadratic Reciprocity Law
  - A.3.1 A Lemma of Gauss
  - A.3.2 Quadratic Reciprocity for Prime Numbers
  - A.3.3 Quadratic Reciprocity for Odd Integers

References

Index

# 《Primality Testing in》

## 版权说明

本站所提供下载的PDF图书仅提供预览和简介，请支持正版图书。

更多资源请访问：[www.tushu000.com](http://www.tushu000.com)