

Contents

1. Introduction: Efficient Primality Testing	1
1.1 Algorithms for the Primality Problem	1
1.2 Polynomial and Superpolynomial Time Bounds	2
1.3 Is PRIMES in P?	6
1.4 Randomized and Superpolynomial Time Algorithms for the Primality Problem	7
1.5 The New Algorithm	9
1.6 Finding Primes and Factoring Integers	10
1.7 How to Read This Book	11
2. Algorithms for Numbers and Their Complexity	13
2.1 Notation for Algorithms on Numbers	13
2.2 O -notation	15
2.3 Complexity of Basic Operations on Numbers	18
3. Fundamentals from Number Theory	23
3.1 Divisibility and Greatest Common Divisor	23
3.2 The Euclidean Algorithm	27
3.3 Modular Arithmetic	32
3.4 The Chinese Remainder Theorem	35
3.5 Prime Numbers	38
3.5.1 Basic Observations and the Sieve of Eratosthenes	39
3.5.2 The Fundamental Theorem of Arithmetic	42
3.6 Chebychev's Theorem on the Density of Prime Numbers	45
4. Basics from Algebra: Groups, Rings, and Fields	55
4.1 Groups and Subgroups	55
4.2 Cyclic Groups	59
4.2.1 Definitions, Examples, and Basic Facts	59
4.2.2 Structure of Cyclic Groups	62
4.2.3 Subgroups of Cyclic Groups	64
4.3 Rings and Fields	66
4.4 Generators in Finite Fields	69

5. The Miller-Rabin Test	73
5.1 The Fermat Test	73
5.2 Nontrivial Square Roots of 1	78
5.3 Error Bound for the Miller-Rabin Test	82
6. The Solovay-Strassen Test	85
6.1 Quadratic Residues	85
6.2 The Jacobi Symbol	87
6.3 The Law of Quadratic Reciprocity	88
6.4 Primality Testing by Quadratic Residues	92
7. More Algebra: Polynomials and Fields	95
7.1 Polynomials over Rings	95
7.2 Division with Remainder and Divisibility for Polynomials	102
7.3 Quotients of Rings of Polynomials	105
7.4 Irreducible Polynomials and Factorization	108
7.5 Roots of Polynomials	111
7.6 Roots of the Polynomial $X^r - 1$	112
8. Deterministic Primality Testing in Polynomial Time	115
8.1 The Basic Idea	115
8.2 The Algorithm of Agrawal, Kayal, and Saxena	117
8.3 The Running Time	118
8.3.1 Overall Analysis	118
8.3.2 Bound for the Smallest Witness r	119
8.3.3 Improvements of the Complexity Bound	120
8.4 The Main Theorem and the Correctness Proof	122
8.5 Proof of the Main Theorem	123
8.5.1 Preliminary Observations	124
8.5.2 Powers of Products of Linear Terms	124
8.5.3 A Field F and a Large Subgroup G of F^*	126
8.5.4 Completing the Proof of the Main Theorem	130
A. Appendix	133
A.1 Basics from Combinatorics	133
A.2 Some Estimates	136
A.3 Proof of the Quadratic Reciprocity Law	137
A.3.1 A Lemma of Gauss	137
A.3.2 Quadratic Reciprocity for Prime Numbers	139
A.3.3 Quadratic Reciprocity for Odd Integers	141
References	143
Index	145

<http://www.springer.com/978-3-540-40344-9>

Primality Testing in Polynomial Time
From Randomized Algorithms to "PRIMES Is in P"
Dietzfelbinger, M.
2004, X, 150 p., Softcover
ISBN: 978-3-540-40344-9