Contents

Preface xi

Introduction 1

Part 1. Foundations

Chapter 1. Natural numbers and primes 13

§1.1. The natural numbers 13

§1.2. Divisibility and primes 26

§1.3. Prime factor decomposition 31

§1.4. The Euclidean algorithm 35

§1.5. The Sieve of Eratosthenes 39

§1.6. There are infinitely many primes 41

Further reading 42

Chapter 2. Algorithms and complexity 43

§2.1. Algorithms 43

§2.2. Decidable and undecidable problems 52

§2.3. Complexity of algorithms and the class **P** 57

§2.4. The class **NP** 68

Bibliografische Informationen
http://d-nb.info/105856157X

digitalisiert durch DEUTSCHE NATIONAL BIBLIOTHEK

§2.5. Randomized algorithms 73
Further reading 81

Chapter 3. Foundations of number theory 83
§3.1. Modular arithmetic 84
§3.2. Fermat's Little Theorem 94
§3.3. A first primality test 104
§3.4. Polynomials 107
§3.5. Polynomials and modular arithmetic 120
Further reading 127

Chapter 4. Prime numbers and cryptography 129
§4.1. Cryptography 129
§4.2. RSA 132
§4.3. Distribution of primes 136
§4.4. Proof of the weak prime number theorem 139
§4.5. Randomized primality tests 143
Further reading 150

Part 2. The AKS Algorithm

Chapter 5. The starting point: Fermat for polynomials 153
§5.1. A generalization of Fermat's Theorem 153
§5.2. The idea of the AKS algorithm 159
§5.3. The Agrawal-Biswas test 163

Chapter 6. The theorem of Agrawal, Kayal, and Saxena 169
§6.1. Statement of the theorem 170
§6.2. The idea of the proof 171
§6.3. The number of polynomials in $\mathcal{P}$ 173
§6.4. Cyclotomic polynomials 178

Chapter 7. The algorithm 183
§7.1. How quickly does the order of n modulo r grow? 183
§7.2. The algorithm of Agrawal, Kayal, and Saxena 186
§7.3. Further comments 189
Further reading 192

Appendix A. Open questions 193
Further reading 205

Appendix B. Solutions and comments to important exercises 207

Bibliography 233

List of symbols 237

Index 239