Preface to the English Edition

The American Mathematical Society has honored me by deciding to translate this book into English.

This book is of a theoretical nature and contains descriptions and proofs of correctness for basic number-theoretic algorithms. It provides an overview of modern algorithmic number theory, including the most recent results.

About 150 new items have been added to the bibliography. Mostly, they are mentioned for reference purposes, without providing detailed descriptions of their results. Many of the added papers can be found in the Cryptology ePrint Archive (`http://www.iacr.org`).

The author is grateful to I. E. Shparlinski for advice and for a number of useful comments on the contents of the book. The author also thanks C. Pomerance and T. Denny for important and interesting papers that they sent to him in the mid-1990s.

Preface

This book deals with algorithmic number theory, a rapidly developing, especially in the last thirty years, branch of number theory, which has important applications to cryptography. Its explosive growth in the 1970s was related to the emergence of the Diffie-Hellman and RSA cryptosystems. By some estimates, practically the entire world arsenal of asymmetric cryptography is based on number-theoretic techniques.

For the needs of cryptography (in terms of practical implementation and security of cryptographic tools, as well as for the development of methods for their breaking) improving the efficiency of the following methods and algorithms becomes critically important:

- algorithms for primality testing of integers;
- factorization methods (i.e., methods for factoring integers);
- computations using elliptic curves over finite fields;
- algorithms for computation of the discrete logarithm;
- factorization methods for polynomials over finite fields and over the rationals;
- methods for solving linear systems over finite fields;
- algorithms for performing arithmetic operations on large integers;
- algorithms for polynomial arithmetic.

In this book we tried to describe the current state of algorithmic number theory, and give sufficiently accurate descriptions of the used algorithms. Some of the more complicated algorithms and methods (such as primality testing using trigonometric sums or the number field sieves) are only mentioned in the form of general schemes. We also tried to provide (in a survey-like manner) many references to the existing literature. An interested reader can augment our list of reference by turning to the monographs [**22, 69**], as well as to the Internet sites `www.cryptography.ru` and `www.math.uga.edu/~ntheory`.

This book is based on the courses in algorithmic number theory that the author gave at the Mathematics and Mechanics Department of Moscow State University from 1993 to 2001. For a number of years, the author also ran seminars on number-theoretic algorithms at MSU and, more recently, the seminar "Number-theoretic algorithms in cryptography" at the chair of information security of the MSU (jointly with the member of the Cryptography Academy of the Russian Federation V. M. Sidelnikov). A number of results mentioned in this book were obtained by the author jointly with the members of the Laboratory of Mathematical Problems of Cryptography at MSU.

This is not a book on elementary mathematics. Reading it requires serious preparation, say, two or three years of studying typical mathematics courses at a university.

We assume that the reader is familiar with number theory, as covered by I. M. Vinogradov's "An introduction to the theory of numbers" (any edition). Some parts of the book require familiarity with continued fractions (see, for example, [**117, 130**]). For the convenience of the reader we collected the basic definitions and facts in the Appendix. Some sections require the basic facts from the theory of finite fields (see, for example, [**153**]) as well as basic algebraic number theory (see, for example, [**261**]). At some places, deeper facts from algebraic number theory are needed; in that case we provide references in the text. Among the textbooks on cryptography we recommend [**11**].

Many algorithms mentioned here use auxiliary algorithms for computing the greatest common divisor of integers and for exponentiation. Such algorithms are well known and can be found in many texts; see, for example, [**118, 57, 22**]. We mention those algorithms in the Appendix, some of them without a proof of correctness.

Whenever we say that an algorithm requires a certain number of arithmetic operations, we mean arithmetic operations (addition, subtraction, multiplication, and division) with large integers (high-precision arithmetic).

The *complexity of an algorithm* is the number of arithmetic operations it performs. Normally, the complexity is represented as a function of the *length of the input*, i.e., of the number N of bits required to store the input. If this function is a polynomial in N, one says that the algorithm has a *polynomial complexity* (*polynomial* algorithm); if this function is of the form $L_N[\gamma; c] = e^{(c+o(1))N^{\gamma}(\log N)^{1-\gamma}}$, where $0 < \gamma < 1$ and $c = \text{const}$, $c > 0$, then the complexity estimate for the algorithm is said to be *subexponential* with exponent γ; if the function is of the form e^{cN}, where $c = \text{const}$, then the algorithm has an *exponential* complexity. For example, let $n \in \mathbb{N}$ and we want to factor n. The length of the input equals $N = [\log_2 n] + 1 = O(\log n)$. Then a polynomial factorization algorithm has complexity $O((\log n)^c)$, a subexponential algorithm has complexity $e^{(c+o(1))(\log n)^{\gamma}(\log\log n)^{1-\gamma}}$, and an exponential algorithm, complexity $O(n^c)$.

We say that a number is *B-smooth* if all of its prime factors are less than or equal to B (here B is a positive number, called the *smoothness boundary*). An integer is said to be *B-power-smooth* if each of its primary factors (the powers of primes) is at most B.

We use the symbol $\log x$ to denote the natural logarithm of the positive number x.

The author is grateful to A. A. Salnikov, V. V. Yashchenko, and D. V. Matyukhin for their help during the work on this book, many discussions, and their advice leading to numerous improvements of the manuscript.

The author also thanks D. V. Matyukhin for the big job of technical editing of the manuscript.