

**io-port 05833178****Nabebin, A. A.****Discrete mathematics.** (Дискретная математика.)

Moskva: Nauchnyĭ Mir (ISBN 978-5-91522-190-0/hbk). 509 p. (2010).

This book is intended as a handbook for students of higher technical schools of specializations like applied mathematics or informatics as well as for students of specializations with extended courses of numerical methods and computer programming. It represents a brief elaboration of extremely numerous subjects. The book includes the following sections: indent=6mm

Introduction. Basic definitions from naive set theory and abstract algebra.

## I. Modular arithmetic

1. Divisibility: prime numbers and Miller-Rabin primality test, Fundamental Theorem of Arithmetic, the greatest common divisor, Euclid's algorithm for finding  $\gcd(n, m)$  and extended Euclidean algorithm, the least common multiple, continued fraction expansion of real numbers (rational and irrational cases).
2. Möbius and Euler functions. Functions: floor, ceiling and fractional part. Multiplicative functions, Möbius function and Möbius inverse formula. Euler phi-function.
3. Congruences – basic properties, complete and the least residue systems, Euler's and Fermat's Theorems, modular arithmetic - three respective algorithms are given.
4. Linear congruences, Chinese Remainder Theorem with Gauss's proof and some generalization, integral polynomial congruences and the Chinese Remainder Theorem for Polynomials. Kurt Hensel's Theorem with application.
5. Quadratic residues – basic properties.
- 5.2 Legendre symbol with ten fundamental properties (given in very applicable manner) including Gauss's and Einstein's Lemmas and the Quadratic Reciprocity Law (for odd prime numbers).
- 5.3 Jacobi symbol and the Quadratic Reciprocity Law (for odd and relatively prime positive integers). Algorithm for computation of the Jacobi and Legendre symbols.
- 5.4 Theorems on solutions for the general quadratic congruences.
6. Exponent, universal exponent, primitive roots of given  $m = p^\alpha, 2p^\alpha, 2$  and  $4$ , indices (discrete logarithms).
7. Groups, rings, fields, rings  $P[x]$  of polynomials in the unknown  $x$  over the field  $P$ , linear spaces, finite fields. Eleven different algorithms on fundamental aspects of this algebraic structures are presented (for example, the ones for finding the multiplicative inverses of elements of  $\mathbb{F}_{p^m}$ , the order of elements of given finite group, the Gauss algorithm).
8. Application of modular arithmetic to cryptography.
  - 8.1 Overview of cryptography and basic notions. Hash function and MASH algorithm.
  - 8.2 Factoring. Three algorithms are given – two Pollard's algorithms: the rho algorithm and the  $p - 1$  factoring algorithm and, as the third one, the quadratic sieve factoring algorithm.
  - 8.3 RSA problem.
  - 8.4 Quadratic residue problem (five algorithms are included in this section).
  - 8.5 Discrete logarithms problem. Three algorithms are given: Baby Step, Giant Step-Shank's algorithm, Pollard's rho algorithm and the Pohlig-Hellman algorithm.
  - 8.6 Subset of the sum problem (with two algorithms).
  - 8.7 Factorization of polynomials over finite fields. Square-free algorithm and Q-matrix Berlekamp's algorithm are discussed here.
  - 8.8 RSA algorithm.
  - 8.9 RSA signatures.
  - 8.10 ElGamal Public Key Cryptosystem.
  - 8.11 ElGamal Signature Scheme.
  - 8.12,13 General ElGamal Cryptosystem and Signature Scheme, respectively, with multiplicative group  $G$  of Galois field  $GF(p^m)$ .
  - 8.14 Digital Signature Algorithm (DSA).
  - 8.15,16,17 Rabin's Cryptosystem and Rabin's Signature Scheme.
  - 8.18 McEliece Cryptosystem.
  - 8.19 Merkle-Hellman knapsack encryption scheme.
  - 8.20 Chor-Rivest knapsack public-key encryption scheme.
  - 8.21 Probabilistic public-key encryption.
  - 8.22,23 Goldwasser-Micali and Bloom-Goldwasser Probabilistic Coding Schemes.
  - 8.24,25,26,27 Feige-Fiat-Shamir Signature Scheme, Guillou-Quisquater (GQ) Signature Scheme, Schnorr and Niberg-Ruppel Signature Schemes.

- 
9. Real recurrence sequences, finite differences, difference equations, linear recurrence sequences (homogenous and nonhomogenous of constant and variable coefficients): solutions, concept of the so-called Casoratian of a set of solutions, Lagrange's method of finding the special solution of nonhomogenous linear recurrence sequence.
  - II. Combinatorics – basic concepts.
  10. Permutations and combinations, choices with repetition, addition principle, multinomial coefficients.
  11. Generating functions (as formal power series), special generating functions for combinations, choices with constraints on repetitions and without any constraints on repetitions.
  12. Principle of inclusion and exclusion with some applications.
  - III. Algebra of logics and predicates.
  13. Logic functions, Boolean functions, formulae, normal forms, minimized normal forms (with six algorithms), minimization of the partially defined functions (the section contains two respective algorithms), dual functions, Zegalkin's polynomial over field  $F$ , Zegalkin's Theorem, linear functions, monotonic functions, Post's Theorem.
  14. Functions of the  $k$ -values logic, monotonic functions (partial orders and Martyniuk's Theorem), linear functions, functions preserving partition, classes of type  $C$  and  $B$ .
  15. Partially ordered sets, Zorn's Lemma, lattices, isomorphisms of lattices, Boolean algebras and Stone's Theorem for the finite Boolean algebras (proof of this one is included).
  16. Logic circuits analysis. Shannon functions (complexity of the boolean minimal realization problem), Lapunov's Theorem, multiplexers.
  17. Logic of predicates, quantifiers, terms, formulae, subformulae, formulae in prenex form (theorem saying that every formula is equivalent in logic of predicates to a formula in prenex form). Church's Theorem. Theorems on decidability of the existential formulae and universal formulae.
  - 17.6–10 Relations, compositions of functions, Malcev's operations over functions, algebra of relations, Post's co-algebra.
  - IV. Graphs and algorithms.
  18. Terminology of graphs, digraphs, Dijkstra algorithm.
  19. Eulerian circuits and graphs, De Bruijn sequences, Hamiltonian circuits and graphs, Gray codes.
  20. Trees and forests (basic notions and facts), spanning trees of connected graphs.
  21. Circuits in graphs, linear space of subgraphs of the given graph, subspace of even subgraphs (cycle space) and induced cycles, cyclomatic number of the given graph, Kirchhoff's Matrix Theorem.
  22. Bipartite graphs. Matching in bipartite graphs: Rado's Theorem (on injective choices) and Hall's Theorem.
  23. Planar graphs: Euler's Formula, proofs of non-planarity of graphs  $K_5$  and  $K_{3,3}$  are presented, Kuratowski's Theorem on Planarity and Petersen Graph, algorithm for finding a plane graph of the given planar graph.
  24. Coloring of graphs. Chromatic number of the graph, lower and upper bounds of chromatic number, bichromatic graphs and five respective algorithms. Five Color Theorem (with Heawood's proof by induction). In my opinion, comments on Four Color Theorem, contained in this section, is insufficient.
  25. Networks and flows. Basic concepts and facts: capacity of the cut in flow network,  $s - t$  flow network, Ford-Fulkerson Theorem.
  - 25.6 Two algorithms for maximum flow (including also Dijkstra algorithm) are presented.
  26. Counting graphs – this section contains, among others, Burnside's Lemma and Polya's Theorem of Counting (both with proofs) and their very interesting applications to the problem of coloring of the set of vertices in the cube.
  - V. Monadic logic and finite automata.
  27. Finite automata, Mealy and Moore models of automata, regular languages and some closure properties of regular languages, minimization of finite automata.
  28. Macroautomata.
  29. Uniformization of finite automata languages.
  30. Monadic logic. In my opinion, Nabebin exposes the subjects in a very good way and in an impressive didactic spirit. From one side he gives to the teacher, and to the student as well, a possibility of completing practically every one of the discussed subjects. From the other side the book assures a sufficient support in each of the fields presented for every reader, for the new students as well as for the experienced readers who intend to quickly refresh some forgotten subjects. In a very good way, I may even say, magnificently, the author deals with mathematical formalism. Presented proofs of selected facts are brief but also clear, like for example the proofs of theorems concerning the elementary number theory, linear recurrence sequences, Boolean algebras etc. Also examples illustrating the discussed problems (theorems, algorithms) are the right ones and reliably chosen. The algorithms (and there is really a lot of them) are explained neatly and simply and, what is interesting, they are very inspiring (while reading the various algorithms I have asked many

times questions to myself about the various additional variants or I have even formulated some new problems in their context). Moreover, the author makes a lot of efforts for introducing to the reader the problems which are almost standard, but they are presented in definitely more general frame. This makes for an additional quality of the book, since it provokes the reader to discussions or possible generalizations. Summarizing, I warmly recommend the book of Nabebin. It is magnificently written by the master of didactics and the excellent mathematician. Remark: A comparison of the book under review with other books on Discrete Mathematics is very difficult, almost impossible. As a last remark I might add that the reader who is more experienced in the abstractive contents of the book can certainly more easily be convinced of its teaching quality.

*Roman Witula (Gliwice)*