Introduction to the Theory of Computing 1

Fall semester 2023

Syllabus

1. (September 4, 5.) Fundamentals of number theory, theorems about primes (1.1). Congruences (1.2).
2. (September 11.) Linear congruences. Simultaneous congruence systems (1.4).
3. (September 18, 19.) Euler-Fermat theorem, little Fermat theorem (1.3). Number theoretic algorithms: basic operations, exponentiation (1.5.1-1.5.3).
4. (September 25, 26.) Euclidean algorithm, its application for solving linear congruences (1.5.4-1.5.5). Primality testing, public key criptography, RSA-encoding (1.5.6-1.5.7).
5. (October 3.) Geometry of 3-space: equations of planes, lines; intersections (2.1).
6. (October 9, 10.) $\mathbb{R}^n$, operations in $\mathbb{R}^n$. Subspaces of $\mathbb{R}^n$. Linear combination, spanned (generated) subspace, generating system (2.2.1-2.2.3).
7. (October 16, 17.) Linear independence. Exchange theorem, I-G inequality (2.2.4-2.2.5).
8. (October 24.) Basis, dimension, standard basis, the dimension of $\mathbb{R}^n$ and its subspaces (2.2.6).
9. (October 30, 31.) Systems of linear equations, Gaussian elimination. Conditions on solvability and uniqueness (2.3). Definition of determinants (2.4.1-2.4.2).
10. (November 3.) First midterm. Material: up to dimension (1.1-2.2).
11. (November 6, 7.) Determinants: ways of evaluation, expansion theorem. Cross product (2.4.3-2.4.7).
12. (November 13, 14.) Matrices, operations on matrices. Product theorem for determinants. Connection between systems of linear equations and matrix equations (2.5.1-2.5.2).
13. (November 20, 21.) Inverse of a matrix, necessary and sufficient condition for its existence, calculation of the inverse. Rank of a matrix (2.5.3-2.5.4).
15. (December 1.) Second midterm. Material: up to rank (2.3-2.5).
16. (December 4, 5.) Changing bases, the matrix of a linear transformation in a given basis. Eigenvalues and eigenvectors of matrices, characteristic polynomial. Diagonalisation (2.6.5-2.6.6).

The numbers in parentheses denote the chapters and sections in the Lecture Notes.