UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

SYLLABUS DEL CORSO

Metodi Algebrici per l'Informatica

2021-2-E3101Q129

Aims

At the end of the course the student is able to apply some results from abstract algebra to analyse and solve problems related to computer science. For instance, the basic rules used in the error-correcting codes, and the basic rules used to guarantee a high level of security in the modern cryptographic systems.

Contents

Introduction to the elementary algebraic structures. Modular arithmetic, finite fields and permutation groups. Brief introduction to cryptography. Coding theory, linear codes and classical examples of linear codes.

Detailed program

Basic Arithmetic. Fondamental theorem of arithmetic. Decomposition of a number in prime factors.

Review of Equivalence Relations. Congruences modulo n. Quotient sets and the example Z/nZ. Review of the basic operations in number field. Algebraic structures.

Algebraic structures: groups and rings. Permutation groups: number of permutations and basic properties of the symmetric group.

The algebraic structure of the ring Z/nZ . Linear congruences and the Chinese remainder theorem. The Euler phi-function and its application to factorization problems.

Generalized Euler's theorem. Introduction on the RSA. Primality tests.

Finite fields: Z_p, with p a prime number.The ring of polynomials in one variable. Construction of finite fields using the polynomial rings.

Introduction to error-correcting codes and linear codes.

Prerequisites

The student is supposed to be familiar with the mathematics studied in High School and with the mathematical contents in the course Fondamenti dell'Informatica

Teaching form

Lectures, exercise classes, personal study supported by the e-learning platform. The course is delivered in italian.

Textbook and teaching resource

Course notes avalaible on the e-learning platform.

Textbooks:

Elementi di Matematica Discreta e Algebra Lineare, Francesca Dalla Volta e Marco Rigoli, Pearson Education.

A Course in Number Theory and Cryptography, Neal Koblinz, Springer Verlag.

Semester

First semester.

Assessment method

Written exam.

The written exam consists in

a) open-ended reasoning questions

b) solving numerical exercises or problems

Mid-term and end of term exams are provided. They consist in

a) open-ended reasoning questions

b) solving numerical exercises or problems

The mid-term and end of term exams substitute the written exam.

Oral exam: optional

Assessment: final mark

Office hours

On appointment.