UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

SYLLABUS DEL CORSO

Metodi Algebrici per l'Informatica

2526-2-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.

1. Knowledge and understanding
   By the end of the course, students will have acquired a foundational understanding of discrete mathematics, focusing on modular arithmetic, congruences, residue classes, basic elements of group theory, and introductory notions of classical cryptography and error-correcting codes.

2. Applying knowledge and understanding
   Students will be able to apply the learned concepts and techniques to solve practical problems and develop solutions in areas related to computer science, such as data security and reliable data transmission.

3. Making judgements
   Students will develop the ability to critically and independently analyze the theoretical concepts, evaluating the correctness and effectiveness of mathematical methods in computing contexts.

4. Communication skills
   Students will be able to clearly and rigorously explain the studied mathematical concepts, using appropriate symbolic and technical language, both in written and oral form.

5. Learning skills
   Students will acquire logical and mathematical tools that enable them to autonomously pursue further learning in advanced topics in mathematics and theoretical computer science.

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.
Brief Introduction to some CAS (Computer Algebra System) e.g. Magma, GAP, gp/pari or Sagemath.

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. Normal subgroups, ideals of a ring, morphisms. 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: F_p, with p a prime number. The ring of polynomials in one variable. Construction of finite fields using 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

Frontal lessons, exercises, individual study supported by e-learning teaching materials. The course is taught in Italian.
The planned activities are: 48 hours of frontal lessons in delivery mode and 20 hours of frontal exercises in delivery mode.

Textbook and teaching resource

Course notes avalaible on the e-learning platform.
Textbooks:
Childs, Lindsay N. "A concrete introduction to higher algebra. Second edition". Undergraduate Texts in Mathematics. Springer-Verlag, New York, 1995.
Koblitz, Neal "A course in number theory and cryptography". Graduate Texts in Mathematics, 114. Springer-Verlag, New York, 1987.
Craven, David "Computing with Magma", https://web.mat.bham.ac.uk/D.A.Craven/docs/lectures/magma.pdf

Semester

First semester.

Assessment method

In order to access the written assessment one has to pass a computer assisted exam.
This requires inscription to the WIMS platform https://wims.matapp.unimib.it/
There 10 tests are available (one for each week of lectures). They will be gradually activated.
Their resolutions will allow you to tune in with the course contents. Moreover the first part of the exam will consist of a few
exercises selected among those of all tests.
There will be no partial assessments.
At the end of the lectures a bonus of xx will be assigned to a yy score according to following table:

- xx=2 if 27<yy?30;
- xx=1.5 if 22<yy?27;
- xx=1 if 18?yy<22.
  The bonus remains valid until the beginning of the following year's course.

The exam is divided into five phases:

1. Multiple choice test to ensure that the basic concepts have been acquired. Here the accuracy of the answers is assessed (max. 10 points)
2. If sufficient, this test gives access to the written test consisting of the resolution of some routine exercises (max. 10 points)
3. Assignment of an exercise in which the ability to rework and use the theory for problem-solving purposes is assessed (max. 6 points)
4. Request to outline one of the key theorems of the course providing hints of demonstration and examples (max. 4 points)
5. Oral exam requires the presentation of assertions and demonstrations of theorems, definitions, examples/counterexamples and calculation techniques.
   It is mandatory for those who obtain a score lower than 21 in the previous phases, optional otherwise;
   for those who obtain a grade >= 27 and do not take the oral exam will be verbalized 27.

No weight is attributed a priori to the oral exam compared to the previous exams.

The first two phases are carried out by accessing the WIMS platform https://wims.matapp.unimib.it/

Office hours

By appointment

Sustainable Development Goals

QUALITY EDUCATION