Universidad Zaragoza

Academic Year/course: 2023/24

27045 - Applied and Computational Algebra

Syllabus Information

Academic year: 2023/24
Subject: 27045 - Applied and Computational Algebra
Faculty / School: 100 - Facultad de Ciencias
Degree: 453 - Degree in Mathematics
ECTS: 6.0
Year: 4
Semester: Second semester
Subject type: Optional
Module:

1. General information

Three applications of algebra have been selected. Groebner bases, which solve problems related to polynomials in several variables. Current cryptography, RSA and methods related to the discrete logarithm problem, in particular based on elliptic curves. Theory of error correcting codes for data transmissions based on linear algebra and finite fields.

The approaches and objectives of this module are aligned with the Sustainable Development Goals (SDGs) of the United Nations 2030 Agenda; the learning activities could contribute to some extent to the achievement of the goals 4 (quality education), 5 (gender equality), 8 (decent work and economic growth), and 10 (reducing inequality).

2. Learning results

- Develop and apply algorithms.
- Appreciate the application of algebra topics in problems of social and technological interest.
- Know in depth the mathematical mechanisms that solve security and authenticity problems in data transmissions.
- Know the power of algorithms derived from Gröbner bases.

3. Syllabus

I. Gröbner bases.
    1. Orderings on the monomials.
    2. Monomial ideals and Dickson's lemma.
    3. Hilbert's basis theorem.
    4. Properties of Gröbner bases.
    5. Applications of the Gröbner bases.

II. Cryptography.
    6. Principles of cryptography.
    7. The Advanced Encryption Standard System (AES).
    8. Public-key cryptography. The RSA cryptosystem.
    9. Public-key cryptosystems based on the discrete logarithm problem.
    10. Elliptic curve cryptosystems.
    11. Electronic signature. The electronic identity card (DNIe).
    12. Hash functions.

III. Error correcting codes.
    13. Error-detector codes.
    14. Linear codes.
    15. The Hamming codes.
    16. Multiple-error correcting codes: BCH codes.
    17. Burst error-correcting codes: the Reed-Solomon codes.

4. Academic activities

Master classes: 45 hours.
Problem solving: 15 hours.
Study: 85 hours.
Assessment tests: 5 hours.

5. Assessment system

- Participation during the development of classes, both theoretical, practical and on the computer.
- Resolution of some problems proposed to present in class.
- Development of computer programs, in which some of the algorithms submitted in class are materialized, and their application to specific cases.
- Written exams of the different parts of the subject.

Each of the three parts of the course will have an independent grade that will be 1/3 of the overall grade. For each part there will be at least one computer practice and a maximum of three. For each part there will be at least one exam before the global exam that will account for 90% of the grade for that part. To pass, it will be necessary to have done all the proposed computer practices and have passed the exams corresponding to the three parts of the subject. The global exam may be used to pass or raise the grade in all or in any of the three parts of the subject.

The LaTeX presentations of some of the proposed exercises will be valued.

Any student will be guaranteed the right to pass the subject by a final comprehensive exam.