Universidad Zaragoza

Academic Year/course: 2021/22

27045 - Applied and Computational Algebra

Syllabus Information

Academic Year: 2021/22
Subject: 27045 - Álgebra aplicada y computacional
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

2. Learning goals

3. Assessment (1st and 2nd call)

3.1. Assessment tasks (description of tasks, marking system and assessment criteria)

The students must demonstrate that they have achieved the expected learning outcomes through the following assessment activities:

1. Participation during the development of classes, both theoretical, practical and on the computer.
2. Resolution of some problems proposed to present in class.
3. Development of computer programs, in which some of the algorithms submitted in class are materialized, and their application to specific cases.
4. 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.

4. Methodology, learning tasks, syllabus and resources

4.1. Methodological overview

The learning process that has been designed for this subject is based on the following:

The theory and problems classes (3 per week) will be used for the presentation and development of the different topics. This development should be later expanded by the student, with the use of notes and adequate bibliography. The development of computer programs will be through two hours every fortnight.

The Moodle tool and email will be used as a form of communication between teacher and student. Sage will be used for the computer practice classes. Texts and notes will be made available to the student to help them follow the course.

4.2. Learning tasks

Attendance and participation in classes.

Some class will be dedicated to solving exercises by students. They must show their communication and reasoning skills, through oral expression.

Writing of the resolution of exercises using LaTeX.

Solving problems using a computer (SAGE program), on a biweekly basis.

Consultation of procedures for solving the previous activities in tutorials.

Search for real life problems related to the contents of the subject.

Teaching and evaluation activities will be carried out in person unless, due to the health situation, the provisions issued by the competent authorities and by the University of Zaragoza decide to carry them out electronically or semi-systematically with reduced rotating capacity.

4.3. Syllabus

Part I. Bases of Gröbner.

1. Orderings on the Monomials.
2. Monomial Ideals and Dickson's Lemma.
3. Properties of Gröbner bases.
4. Applications of the Gröebner bases.

Part II. Cryptography.

1. Principles of cryptography.
2. The Advanced Encryption Standard System (AES).
3. Public-key cryptography. The RSA Cryptosystem.
4. Public-Key Cryptosystems based on the Discrete Logarithm Problem.
5. Elliptic Curve Cryptosystems.
6. Electronic Signature. The Electronic Identity Card (DNIe).
7. Hash Functions.

Part III. Error correcting codes.

1. Error-Detector Codes.
2. Linear Codes.
3. The Hamming Codes.
4. Multiple-Error Correcting Codes: BCH Codes.
5. Error Burst Correcting Codes: The Reed-Solomon Codes.

4.4. Course planning and calendar

Information concerning the timetable, classroom, tutorial hours, assessment dates and other details regarding this course will be provided on the first day of class or please refer to the Faculty of Sciences website and Moodle.

4.5. Bibliography and recommended resources

- Hardy, Darel W.. Applied algebra : codes, ciphers, and discrete algorithms / Darel W. Hardy, Fred Richman, Carol L. Walker . - 2nd ed. Boca Raton : Chapman & Hall/CRC, cop. 2009.
- Pastor Franco, José. Criptografía digital : fundamentos y aplicaciones / José Pastor Franco, Miguel Angel Sarasa López, José Luis Salazar Riaño . - 2a. ed. Zaragoza : Prensas Universitarias de Zaragoza, 2001.
- Durán Díaz, Raúl. El criptosistema RSA / Raúl Durán Díaz, Luis Hernández Encinas, Jaime Muñoz Masqué Madrid : Ra-Ma, D.L. 2005.
- Klima, Richard. E. [et al.]. Applications of abstract algebra. With Maple and MATLAB . 2nd. Ed. Taylor & Francis. 2006.
- Joyner, David. Applied Abstract Algebra. Johns Hopkins. 2004.
- Vaudenay, Serge. A Classical Introduction To Cryptography. reprint of 1st ed. 2006 Springer. 2010.
- Paar, Christof. Understanding Cryptography. Springer. 2010.
- Huppert, Bertram. Lineare Algebra. 2ª ed. Vieweg+teubner Verlag. 2010.

http://psfunizar10.unizar.es/br13/egAsignaturas.php?codigo=27045