27045 - Applied and Computational Algebra

Información del Plan Docente

Academic Year	2018/19
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

1.1.Aims of the course

1.2.Context and importance of this course in the degree

1.3.Recommendations to take this course

2.Learning goals

2.1.Competences

2.2.Learning goals

2.3.Importance of learning goals

3.Assessment (1st and 2nd call)

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

4.Methodology, learning tasks, syllabus and resources

4.1.Methodological overview

Course: **Applied and Computational Algebra (degree in Mathematics)**

Objectives: The goal of that course is to show the power of algebra and number theory in the real world. We concentrate on concret objects like groups of points on elliptic curves, polinomial rings and finite fields. We show their applicability to various problems to information handling. Among the applications are cryptographie, electronic signature and error-correcting codes.

27045 - Applied and Computational Algebra

4.2.Learning tasks

The theory lectures (two per week) will be in use for the presentation and development of the different topics. This development will have to be extended later for the student, with the use of notes and suitable bibliography. The resolution of exercises will be realized in weekly class, and the production of computer programs by means of two hours every two weeks. The tool Moodle and e-mail will be in use as a form of communication between teacher and student. For the classes of practices of computer Sage will be in use. It will put at the disposal of the student on texts and notes that help in the follow-up of the subject.

4.3.Syllabus

Course: **Applied and Computational Algebra (degree in Mathematics)**

Programe

Part I. Cryptography

- 1. Introduction to the cryptography.

- 2. The Advanced Enryption Standard (AES).

- 3. Public-Key Criptography. The RSA Cryptosystem

- 4. Public-Key Cryptosystems based on the Discrete Logarithm Problem.

- 5. Ellitic Curve Cryptosystems.

- 6. Electronic Signature. The Electronic Identitie Card (DNIe).

- 7. Hash Functions.

-

Part II. Error-Correcting Codes

- 8. Error-Dectector Codes.

- 9. Linear Codes.

- 10. Encoding and Decoding..

- 11. Perfect Codes. The Hamming Codes.

27045 - Applied and Computational Algebra

- 12. Multiple-Error Correcting Codes: BCH Cides.

- 13. Error Burst Correcting Codes: The Reed-Solomon Codes.

- 14. Error Correction in RS Codes.

- 15. Applications of Error-Correcting Codes.

-

Part III. Computational Algebra

- 16. Introduction to Gröbner.

4.4.Course planning and calendar

Duration: One-semester course of6 credits

Time-line: Wednesday at 10:00-11:00 and Thursday 9:00-11:00.

Computer practices: Wednesday 16:00-18:00, using SAGE and PGP.

4.5.Bibliography and recommended resources

References

- Durán-Hernández-Muñoz, *El criptosistema RSA*, RA-MA, 2005.

- Hardy-Richman-Walker, *Applied Algebra: codes, ciphers and discrete algorithms*, CRC Press, 2009

- Joyner-Kreminski-Turisco, *Applied Abstract Algebra*, Hopkins UP, 2004.

- Klima-Sigmon-Stitzinger, *Applications of Abstract Algebra*, CRC Press, 2000.

- Lidl-Pilz, *Applied Abstract Algebra*, Springer, 1997.

- Paar-Pelzl, *Understanding Cryptography*, Springer, 2010.

- Pastor-Sarasa-Salazar, *Criptografía digital*, Prensas Universitarias de Zaragoza, 2ª ed, 2001.

27045 - Applied and Computational Algebra

- Slinko, Arkadii, *Algebra for Applications*, Springer, 2015.

- Stein, W, *Elementary Number Theory: Primes, Congruences, and Secrets,* 2011, http://wstein.org/ent/ent.pdf