SUBJECT TEACHING GUIDE

G116 - Computational Algebra

Double Degree in Physics and Mathematics
Degree in Mathematics
Degree in Mathematics

Academic year 2024-2025

1. IDENTIFYING DATA					
Degree	Double Degree in Physics and Mathematics Degree in Mathematics Degree in Mathematics			Type and Year	Optional. Year 5 Optional. Year 4
Faculty	Faculty of Sciences				
Discipline	Subject Area: Further Computational Mathematics Mention in Pure and Applied Mathematics				
Course unit title and code	G116 - Computational Algebra				
Number of ECTS credits allocated	6	Term		Semester based (2)	
Web	https://sites.google.com/view/ujuetayo/teaching				
Language of instruction	Spanish	English Friendly	No	Mode of delivery	Face-to-face

Department	DPTO. MATEMATICAS, ESTADISTICA Y COMPUTACION
Name of lecturer	DANIEL SADORNIL RENEDO
E-mail	daniel.sadornil@unican.es
Office	Facultad de Ciencias. Planta: + 3. DESPACHO DANIEL SADORNIL RENEDO (3003D)
Other lecturers	

3.1 LEARNING OUTCOMES
- Know open problems and current challenges in the area of algebra.
- Apply efficient algorithms to determine if a number is prime.
- Recognize cryptography in some protocols.

4. OBJECTIVES

Apply knowledge of group and field theory to primality and factorization tests
Show a historical overview of encryption systems and their evolution.

6. SUBJECT PROGRAM

CONTENTS	
1	Groups, Rings and Finite Fields. Legendre symbol and recyprocity law. Some notions of computational complexity
2	Primality and integer factorisation
3	Cryptography, Private and public Key. Protocols

7. ASSESSMENT METHODS AND CRITERIA

Description	Type	Final Eval.	Reassessn	%
Final Exam	Written exam	Yes	Yes	50,00
Partial Exam	Written exam	No	Yes	50,00
TOTAL				100,00

Observations

Final exam consist in two parts. one corresponding to the partial exam and one of the rest.
Students who have passed the partial exam or have obtained a grade higher than 4, will only have the obligation to take the final exam for the rest of the subject.
In addition, they may also repeat the part corresponding to the partial if they wish to improve the grade. In this case, to obtain the final grade, the average between the two parts will be calculated, using the grade obtained in the last exam.
Students who have obtained a grade lower than 4 in the partial must take both parts of the final exam. Your overall grade will be the arithmetic mean of the marks obtained in each of the two parts of the final exam.
The extraordinary call will have the same characteristics as the ordinary.

Observations for part-time students

Evaluation for partial time students will be the same as other students.

8. BIBLIOGRAPHY AND TEACHING MATERIALS

BASIC

R. Crandall y C. Pomerance. Prime Numbers; A computacional Perspective. Springer 2005.

Von zur Gathen, J., y Gerhard, J. Modern Computer Algebra (3rd ed.). Cambridge University Press. 2013

A. Fuster. et al. Técnicas Criptográficos de Protección de Datos, Ra-Ma. 2000.