Facultad de Ciencias

GUÍA DOCENTE DE LA ASIGNATURA

G116 - Álgebra Computacional

Doble Grado en Física y Matemáticas
Optativa. Curso 5

Grado en Matemáticas
Optativa. Curso 4

Curso Académico 2023-2024

1. DATOS IDENTIFICATIVOS					
Título/s	Doble Grado en Física y Matemáticas Grado en Matemáticas			Tipología y Curso	Optativa. Curso 5 Optativa. Curso 4
Centro	Facultad de Ciencias				
Módulo / materia	MATERIA AMPLIACIÓN DE MATEMÁTICA COMPUTACIONAL MENCIÓN EN MATEMÁTICA PURA Y APLICADA				
Código y denominación	G116 - Álgebra Computacional				
Créditos ECTS	6	Cuatrimestre		Cuatrimestral (2)	
Web	https://sites.google.com/view/ujuetayo/teaching				
Idioma de impartición	Español	English friendly	No	Forma de impartición	Presencial

Departamento	DPTO. MATEMATICAS, ESTADISTICA Y COMPUTACION
Profesor responsable	DANIEL SADORNIL RENEDO
E-mail	daniel.sadornil@unican.es
Número despacho	Facultad de Ciencias. Planta: + 3. DESPACHO DANIEL SADORNIL RENEDO (3003D)
Otros profesores	

2. CONOCIMIENTOS PREVIOS

Las asignaturas de Estructuras Algebraicas, Teoría de Galois y Álgebra Conmutativa.

3. COMPETENCIAS GENÉRICAS Y ESPECÍFICAS DEL PLAN DE ESTUDIOS TRABAJADAS
Competencias Genéricas
(Autonomía) Aprender de manera autónoma nuevos conocimientos y técnicas.
(Buscar información) Utilizar herramientas de búsqueda de recursos bibliográficos y de Internet.
(Leer) Leer textos científicos escritos tanto en español como en inglés.
(Aplicar) Saber aplicar los conocimientos matemáticos a su trabajo o vocación de una forma profesional y poseer las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro del área de las Matemáticas.
(Comunicar) Poder transmitir información, ideas, problemas y soluciones del ámbito matemático a un público tanto especializado como no especializado.
Competencias Específicas
(Conocer demostraciones) Conocer demostraciones rigurosas de algunos teoremas clásicos en distintas áreas de la Matemática.
(Modelizar) Proponer, analizar, validar e interpretar modelos de situaciones reales sencillas, utilizando las herramientas matemáticas más adecuadas a los fines que se persigan.
(Comprender) Comprender y utilizar el lenguaje matemático.
(Resolver) Resolver problemas de Matemáticas, mediante habilidades de cálculo básico y otros, planificando su resolución en función de las herramientas de que se disponga y de las restricciones de tiempo y recursos.
Competencias Básicas
Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio.
Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.
Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.

3.1 RESULTADOS DE APRENDIZAJE
- Conocer problemas abiertos y retos actuales en el área del álgebra.
- Aplicar algoritmos eficientes para decidir si un número es primo y algunos algoritmos de factorización de enteros.
- Cifrar y descifrar datos usando diferentes métodos. -Reconocer el uso de la criptografía en diversos protocolos

4. OBJETIVOS
Aplicar los conocimientos de teoria de grupos y cuerpos a los tests de primalidad y factorización
Mostrar una panorámica histórica de los sistemas de cifrado y su evolución.

5. MODALIDADES ORGANIZATIVAS Y MÉTODOS DOCENTES	
ACTIVIDADES	HORAS DE LA ASIGNATURA
ACTIVIDADES PRESENCIALES	
HORAS DE CLASE (A)	
- Teoría (TE)	30
- Prácticas en Aula (PA)	30
- Prácticas de Laboratorio Experimental(PLE)	
- Prácticas de Laboratorio en Ordenador (PLO)	
- Prácticas Clínicas (CL)	
Subtotal horas de clase	60
ACTIVIDADES DE SEGUIMIENTO (B)	
- Tutorías (TU)	8
- Evaluación (EV)	7
Subtotal actividades de seguimiento	15
Total actividades presenciales (A+B)	75
ACTIVIDADES NO PRESENCIALES	
Trabajo en grupo (TG)	
Trabajo autónomo (TA)	75
Tutorías No Presenciales (TU-NP)	
Evaluación No Presencial (EV-NP)	
Total actividades no presenciales	75
HORAS TOTALES	150

6. ORGANIZACIÓN DOCENTE

CONTENIDOS		TE	PA	PLE	PLO	CL	TU	EV	TG	TA	TU-NP	EV-NP	Semana
1	Introducción. Reciprocidad cuadrática. Nociones de complejidad computacional	6,00	6,00	0,00	0,00	0,00	2,00	1,00	0,00	15,00	0,00	0,00	1-2
2	Primalidad y Factorización de enteros.	12,00	12,00	0,00	0,00	0,00	3,00	3,00	0,00	30,00	0,00	0,00	3-9
3	Criptografía. Clave privada y clave pública. Protocolos.	12,00	12,00	0,00	0,00	0,00	3,00	3,00	0,00	30,00	0,00	0,00	10-15
TOTAL DE HORAS		30,00	30,00	0,00	0,00	0,00	8,00	7,00	0,00	75,00	0,00	0,00	

Esta organización tiene carácter orientativo.

TE	Horas de teoría
PA	Horas de prácticas en aula
PLE	Horas de prácticas de laboratorio experimental
PLO	Horas de prácticas de laboratorio en ordenador
CL	Horas de prácticas clínicas
TU	Horas de tutoría
EV	Horas de evaluación
TG	Horas de trabajo en grupo
TA	Horas de trabajo autónomo
TU-NP	Tutorías No Presenciales
EV-NP	Evaluación No Presencial

7. MÉTODOS DE LA EVALUACIÓN

Descripción	Tipología	Eval. Final	Recuper.	%
Examen final	Examen escrito	Sí	Sí	50,00

Calif. mínima	4,00
Duración	4 horas
Fecha realización	A determinar por la Facultad
Condiciones recuperación	En la convocatoria Extraordinaria
Observaciones	Realización de cuestiones, ejercicios y problemas que versen sobre los tópicos tratados en la asignatura. Se dividirá en dos sesiones: en la primera, se realizará el examen correspondiente a la materia no evaluada en el examen parcial la segunda corresponderá a la misma materia del parcial. Se presentarán a ella los que no hayan obtenido la nota mínima y aquellos que deseen modificar su calificación en esta parte. En este caso la calificación será la obtenida en este examen.

Examen parcial	Examen escrito	No	Sí	50,00

Calif. mínima	4,00
Duración	2 horas
Fecha realización	En torno a la semana 10.
Condiciones recuperación	Se podrá recuperar en el examen final
Observaciones	Realización de cuestiones, ejercicios y problemas que versen sobre los tópicos tratados en la asignatura. El alumno que obtenga en este examen una calificación no inferior a 4 podrá presentarse en la convocatoria ordinaria (o en la extraordinaria) solamente a la parte correspondiente a los contenidos restantes.

TOTAL	100,00

Observaciones

El examen final se dividirá en dos partes: la parte correspondiente a la materia del examen parcial y el resto de la materia.

Los alumnos que tengan aprobado el examen parcial o hayan obtenido una nota superior a 4, solamente tendrán la obligación de examinarse en el examen final del resto de la materia.
Además, podrán repetir también la parte correspondiente al parcial si desean mejorar la nota. En este caso, para obtener la nota final, se calculará la media entre las dos partes, utilizando para ello la nota obtenida en el último examen.
Los alumnos que en el parcial hayan obtenido una nota inferior a 4 deben presentarse a las dos partes del examen final. Su calificación global será la media aritmética de las notas obtenidas en cada una de las dos partes del examen final.
La convocatoria extraordinaria tendrá las mismas características que la convocatoria ordinaria.

Criterios de evaluación para estudiantes a tiempo parcial

Las mismas condiciones que para el resto de los alumnos

8. BIBLIOGRAFÍA Y MATERIALES DIDÁCTICOS

BÁSICA

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.

Complementaria

H. Riesel. Prime numbers and computer methods for factorization. Birkhauser. 1985.

D. Stinson. Cryptography : theory and practice. Chapman & Hall. 2006.

9. SOFTWARE

PROGRAMA / APLICACIÓN	CENTRO	PLANTA	SALA	HORARIO

10. COMPETENCIAS LINGÜÍSTICAS

- ☐ Comprensión escrita
- ☐ Comprensión oral
- ☐ Expresión escrita
- ☐ Expresión oral
- ☐ Asignatura íntegramente desarrollada en inglés

Observaciones