Álgebra Algorítmica y Criptografía

Grado en Matemáticas Aplicadas

UNIVERSIDAD NEBRIJA

GUÍA DOCENTE

Asignatura: Álgebra Algorítmica y Criptografía

Titulación: Grado en Matemáticas Aplicadas

Carácter: Obligatoria

Idioma: Castellano

Modalidad: Presencial

Créditos: 6

Curso: 3º

Semestre: 2º

Profesores/Equipo docente: D. Álvaro Pereira Albert

1. COMPETENCIAS Y RESULTADOS DE APRENDIZAJE

1.1. Competencias

Competencias básicas

- CB1, CB2, CB3, CB4, CB5.

Competencias generales

- CG1. (Conocer) Demostrar poseer y comprender, a partir de la base de la educación secundaria, la naturaleza, conceptos, métodos y resultados más relevantes de los diferentes campos de las Matemáticas.
- CG2. (Aplicar) Saber aplicar los conocimientos adquiridos en la definición y planteamiento de problemas y en la búsqueda de sus soluciones en contextos matemáticos y no matemáticos.
- CG5. (Aprender) Haber desarrollado aquellas habilidades de aprendizaje necesarias para emprender, con un alto grado de autonomía, posteriores estudios especializados en el campo de las matemáticas o en cualquier otra disciplina que requiera conocimientos de matemáticas.

Competencias transversales

- CT1. (Comunicar) Comunicar de forma oral o escrita información, ideas, problemas y soluciones a un público tanto especializado como no especializado.
- CT5. (Trabajar en equipo) Saber trabajar en equipo contribuyendo de forma activa al resultado de problema o proyecto a resolver.
- CT6. (Autonomía) Aprender de manera autónoma nuevos conocimientos y técnicas para adaptarse a nuevas situaciones en el entorno de las Matemática Aplicadas u otros.

Competencias específicas:

- CE1. (Comprender) Comprender el lenguaje matemático para utilizarlo con soltura.
- CE2. (Asimilar) Relacionar la definición de nuevos objetos matemáticos con otros conocidos para asimilarlos y deducir sus propiedades.
- CE3. (Demostrar) Identificar las ideas esenciales de las demostraciones de algunos teoremas básicos sabiéndolas adaptar para obtener otros resultados.
- CE4. (Abstraer) Saber abstraer las propiedades estructurales, distinguiéndolas de aquellas puramente ocasionales, para formular hipótesis y saber confirmarlas o refutarlas.
- CE5. (Resolver) Adquirir las técnicas y herramientas matemáticas adecuadas para planificar la resolución de problemas de matemáticas.
- CE6. (Modelizar) Utilizar las herramientas matemáticas más adecuadas a los fines que se persigan para proponer, analizar, validar e interpretar modelos matemáticos sencillos.
- CE7. (Instrumentalizar) Utilizar aplicaciones informáticas adecuadas para experimentar en matemáticas, resolver problemas y manejar modelos matemáticos.

1.2. Resultados de aprendizaje

El estudiante al finalizar esta materia deberá:

- Comprender los conceptos básicos de la teoría de grupos, de anillos y de cuerpos.
- Comprender, demostrar y utilizar los teoremas fundamentales de la teoría de anillos y de cuerpos.
- Saber intepretar estos teoremas con soltura los en ejemplos más usuales de este tipo de estructuras, en particular anillos de polinomios y cuerpos finitos.
- Comprender y relacionar los conceptos y propiedades básicas de la Teoría Galois, analizar dichas propiedades en casos abstractos sencillos o en ejemplos concretos, y realizar demostraciones de algunas propiedades teóricas.
- Conocer problemas abiertos y retos actuales en el área del álgebra.
- Comprender algorítmos básicos en anillos de polinomios y su complejidad.
- Conocer y saber aplicar algoritmos eficientes para decidir si un número es primo.
- Conocer las clases de complejidad P y NP.
- Cifrar y descifrar datos usando diferentes métodos.
- Reconocer el uso de la criptografia en diversos protocolos.
- Conocer diferentes tipos de software para álgebra algorítmica y manejar alguno de ellos.

2. CONTENIDOS

2.1. Requisitos previos

Haber cursado Estructuras Algebraicas.

2.2. Descripción de los contenidos

Algoritmos básicos en álgebra y su complejidad. Test de primalidad. Jerarquía de complejidad de problemas, P versus NP. Introducción a la criptografía. Criptografía de clave privada y de clave pública. Blockchain. Códigos.

2.3. Contenido detallado

Presentación de la asignatura

Explicación de la **guía docente**

- **Algoritmos y complejidad.**
  - **Algoritmos básicos en álgebra. Complejidad de un algoritmo. Cálculo de la complejidad. Jerarquía de la complejidad de un algoritmo. P versus NP. Test de primalidad**
- **Introducción a la criptografía.**
  - **Objetivos de la criptografía. Análisis criptográfico. Criptosistemas simétricos o de clave privada.**
- **Criptografía de clave pública.**
  - **Criptosistemas asimétricos. Clave pública. RSA.**
- **Blockchain.**
  - **Cadenas de bloques. Criptografía en las cadenas de bloques.**
- **Teoría de códigos**
  - **Introducción a la teoría de códigos. Códigos correctores de errores. Códigos lineales. Códigos cíclicos.**

2.4. Actividades dirigidas

Durante el curso se realizarán varias actividades dirigidas en forma de trabajos orientados al aprendizaje y aplicación de los nuevos conceptos aprendidos o ampliación de éstos. La actividad formativa “Prácticas” será el marco para establecer contenido y desarrollo de estas actividades que los estudiantes completaran de forma individual o en grupo. Así mismo se trabajará con diferentes paquetes de software especializado. La entrega y la asistencia a las actividades y/o prácticas es obligatoria. La falta de asistencia a una práctica conlleva automáticamente el suspenso de la asignatura en caso de que la ausencia no esté debidamente justificada.

2.5 Actividades formativas

CÓDIGO	ACTIVIDAD FORMATIVA	HORAS	PORCENTAJE DE PRESENCIALIDAD
AF1	Clases de teoría y problemas	45	100%
AF2	Tutorías	15	70%
AF3	Prácticas	9	100%
AF4	Estudio individual y trabajo autónomo	72	0%
AF5	Trabajos individuales o en grupo	12	0%
AF6	Evaluación	6	100%

3. SISTEMA DE EVALUACIÓN

3.1. Sistema de calificaciones

El sistema de calificaciones (R.D. 1125/2003, de 5 de septiembre) será el siguiente:

0 - 4,9 Suspenso (SS)

5,0 - 6,9 (Aprobado (AP)

7,0 - 8,9 Notable (NT)

9,0 - 10 Sobresaliente (SB)

La mención de «Matrícula de Honor» podrá ser otorgada a alumnos que hayan obtenido una calificación igual o superior a 9,0. Su número no podrá exceder del cinco por ciento de los alumnos matriculados en una materia en el correspondiente curso académico, salvo que el número de alumnos matriculados sea inferior a 20, en cuyo caso se podrá conceder una sola «Matrícula de Honor».

3.2. Criterios de evaluación

Convocatoria ordinaria

Sistemas de evaluación	Porcentaje
SE1 Prueba parcial	20%
SE2 Examen final	50%
SE3 Presentación de trabajos	30%

Convocatoria extraordinaria

Sistemas de evaluación	Porcentaje
SE2 Examen final	70%
SE3 Presentación de trabajos	30%

3.3. Restricciones

Calificación mínima

Las ponderaciones anteriores sólo se aplicarán si el alumno/a obtiene al menos un 4 en el examen final.

Es imprescindible la entrega de todos los trabajos y prácticas propuestas en la asignatura. Para poder hacer media de los trabajos/prácticas es necesario obtener en cada uno de ellos una nota igual o superior a 3.5 puntos, y la nota media de todos los trabajos/prácticas deber ser superior o igual a 5. La no superación de los trabajos/prácticas supone el suspenso automático de la asignatura. ponderación tanto del examen parcial como de los conceptos de participación y trabajos escritos/prácticas, sólo se aplicará si el alumno obtiene al menos un 4 en el examen final.

La convocatoria extraordinaria consiste en un examen sobre los contenidos de la asignatura desarrollados en las clases de teoría y problemas. Este examen pondera un 70%, el resto de la nota final corresponde a la calificación de las entregas de trabajos evaluables solicitados durante el periodo docente. Si estos trabajos están suspensos en la convocatoria ordinaria, pueden ser recuperados en convocatoria extraordinaria previa petición del estudiante al profesor. Esta petición se debe realizar por escrito en un plazo máximo de 10 días después de la publicación de la nota final de la convocatoria ordinaria. Esta ponderación también se aplica sólo en el caso de que el alumno obtenga al menos un 4 en este examen final.

Asistencia

El alumno que, injustificadamente, deje de asistir a más de un 25% de las clases presenciales podrá verse privado del derecho a examinarse en la convocatoria ordinaria.

Normas de escritura

Se prestará especial atención en los trabajos, prácticas y proyectos escritos, así como en los exámenes tanto a la presentación como al contenido, cuidando los aspectos gramaticales y ortográficos. El no cumplimiento de los mínimos aceptables puede ocasionar que se resten puntos en dicho trabajo.

3.4. Advertencia sobre plagio

La Universidad Antonio de Nebrija no tolerará en ningún caso el plagio o copia. Se considerará plagio la reproducción de párrafos a partir de textos de auditoría distinta a la del estudiante (Internet, libros, artículos, trabajos de compañeros…), cuando no se cite la fuente original de la que provienen. El uso de las citas no puede ser indiscriminado. El plagio es un delito.

En caso de detectarse este tipo de prácticas, se considerará Falta Grave y se podrá aplicar la sanción prevista en el Reglamento del Alumno.

4. BIBLIOGRAFÍA

Bibliografía básica

- Plaza Martín, F.J., *Manual de criptografía: Fundamentos matemáticos de la criptografía para un estudiante de grado*. Ediciones Universidad de Salamanca, 2021. Disponible online en: https://eusal.es/eusal/catalog/book/978-84-1311-463-7

Bibliografía para prácticas

- García, M.A., Martínez, L., Ramírez, T., *Introducción a la Teoría de Códigos*. Universidad del País Vasco, 2017. Disponible online en: https://ocw.ehu.eus/pluginfile.php/50556/mod_page/content/35/Resumen_total_con_portada.pdf

Bibliografía complementaria

- Guruswami, V., Rudra, A., Sudan, M., *Essential Coding Theory*. University at Buffalo, SUNY, 2023. Disponible en https://cse.buffalo.edu/faculty/atri/
- Lobillo, F.J., *Apuntes de Criptogafía*. Universidad de Granada, 2019. Disponible online en: https://digibug.ugr.es/handle/10481/60106
- del Río Mateos, Á., *Introducción a la critografía*. Universidad de Murcia, 2021. Disponible online en: https://www.um.es/adelrio/Docencia/Criptografia/Criptografia.php