FICHA IDENTIFICATIVA

Datos de la Asignatura

Código	44085
Nombre	Métodos algebraicos y sus aplicaciones
Ciclo	Máster
Créditos ECTS	3.0
Curso académico	2023 - 2024

Titulación(es)

Titulación	Centro	Curso	Periodo
2183 - M.U. en Investigación Matemática 13-V.1	Facultad de Ciencias Matemáticas	1	Segundo cuatrimestre

Materias

Titulación	Materia	Caracter
2183 - M.U. en Investigación Matemática 13-V.1	4 - Intensificación matemática fundamental	Optativa

RESUMEN

Esta asignatura permite al alumno adquirir unas competencias relativas a la aplicación del Álgebra abstracta tanto dentro la matemática pura y aplicada como en otros ámbitos interdisciplinares: ingeniería, informática, ciberseguridad, tratamiento de la información, etc.

Los contenidos de la asignatura hacen referencia a la aplicación de estructuras algebraicas básicas (semigrupos, grupos, anillos, cuerpos, algebras, etc.) en criptografía, teoría de códigos correctores de errores, geometría algebraica, esquemas de reparto de secretos, resolución de sistemas de ecuaciones diferenciales lineales, factorización de números enteros, tests de primalidad, firma digital, resolución de puzzles y sudokus, programación lineal entera, y otras áreas.

CONOCIMIENTOS PREVIOS

Relación con otras asignaturas de la misma titulación

No se han especificado restricciones de matrícula con otras asignaturas del plan de estudios.

Otros tipos de requisitos

Se recomiendan nociones básicas de las siguientes estructuras algebraicas: grupos, anillos, cuerpos y espacios vectoriales.

COMPETENCIAS

2183 - M.U. en Investigación Matemática 13-V.1

- Que los estudiantes comprendan los conceptos y las demostraciones rigurosas de teoremas fundamentales de alguna de las áreas específicas de las Matemáticas.
- Que los estudiantes sean capaces de aplicar los resultados y técnicas aprendidas para la resolución de problemas complejos de alguna de las áreas de las Matemáticas, en contextos académicos o profesionales.
- Que los estudiantes posean la capacidad para enunciar y verificar proposiciones en alguna de las áreas de las Matemáticas y para transmitir los conocimientos matemáticos adquiridos, oralmente y por escrito.
- Que los estudiantes sepan elegir y utilizar herramientas informáticas adecuadas para abordar problemas relacionados con las Matemáticas y sus aplicaciones.

RESULTADOS DE APRENDIZAJE

Las actividades a desarrollar por parte del alumno son un portafolio (resolución de problemas) y un trabajo grupal con los que se valora la capacidad comunicativa en ámbito de la asignatura tanto a nivel escrito como oral. Se realizarán exposiciones orales de los trabajos realizados de forma individual y/o grupal para evaluar la competencia transversal.

DESCRIPCIÓN DE CONTENIDOS

1. Aritmética modular y aplicaciones.

- Conceptos básicos de aritmética modular.
- Aplicaciones de la aritmética modular en criptografía y otros campos.
- Introducción al sistema de álgebra computacional GAP.

2. Teoría de grupos y aplicaciones.

- Revisión de conceptos básicos en Teoría de grupos.
- Teoría de grupos con GAP. El grafo de Cayley.
- Aplicaciones a la resolución de puzzles, geometría y otras áreas.

3. Teoría de anillos y cuerpos. Aplicaciones.

- Revisión de los conceptos básicos de la Teoría de anillos y cuerpos.
- Introducción a la geometría algebraica.
- Cuerpos finitos. Tratamiento con GAP.
- Criptografía basada en el problema del logaritmo discreto: ElGamal y criptografía elíptica.Tratamiento con el sistema computacional Sage.
- Aplicaciones: factorización de números enteros, esquemas de reparto de secretos, tests de primalidad y algoritmos de firma digital.
primalidad y algoritmos de firma digital

4. Introducción a la Teoría de códigos correctores de errores.

- Conceptos básicos: transmisión de la información, código corrector, parámetros.
- Códigos lineales. Codificación. Descodificación con síndromes. Tratamiento con GAP.
- Cotas de los parámetros.
- Códigos de Reed-Solomon

5. Anillos de polinomios. Bases de Groebner y aplicaciones.

- Resultados básicos. Órdenes monomiales. Algoritmo de la división.
- Bases de Groebner.
- Utilización del sistema de álgebra computacional Singular para el cálculo y manejo de las bases de Groebner.
- Aplicaciones: Geometría algebraica, álgebra conmutativa, resolución de ecuaciones en derivadas parciales, programación lineal entera, demostración automática de teoremas geométricos, resolución de sudokus, etc.

VOLUMEN DE TRABAJO

ACTIVIDAD	Horas	% Presencial
Clases de teoría	30,00	100
Elaboración de trabajos en grupo	20,00	0
Elaboración de trabajos individuales	20,00	0
Estudio y trabajo autónomo	5,00	0
TOTAL	**75,00**	

METODOLOGÍA DOCENTE

Se realizará una breve introducción teórica al comienzo de cada tema de la asignatura y posteriormente se analizarán los métodos necesarios para la resolución de las diferentes aplicaciones planteadas relacionadas con los contenidos expuestos en el tema. Se hará uso de diferentes sistemas computacionales algebraicos que ayuden en la resolución de los ejercicios prácticos planteados.

EVALUACIÓN

La evaluación del alumno será continua y estará basada principalmente en la entrega de problemas sencillos mediante la elaboración del portafolio y la realización de un trabajo académico. Se realizará un examen oral para valorar el conocimiento adquirido tanto en el portafolio como en el trabajo académico. A los alumnos que tengan la dispensa de asistir a clase se les plantearán cuestiones sencillas de seguimiento. Se evaluarán con un 80% los trabajos académicos y el portafolio y con 20% la exposición oral y escrita del trabajo realizado.

REFERENCIAS

Básicas

- Applied abstract algebra (Lidl, Rudolf ; Pilz, Günter)
- Modern algebra with applications (Gilbert, William J.)
- Finite group theory (Isaacs, I. Martin)
- Álgebra : a graduate course (Isaacs, I. Martin)
- Applied modern algebra (Larry L. Dornhoff, Franz E. Hohn)
- Applied abstract algebra (Kim, Ki Hang)
- The theory of finite groups : an introduction (Kurzweil, Hans)
- Modern computer algebra (Gathen, Joachim von zur)
- A Singular Introduction to Commutative Algebra [electronic resource] (Greuel, GM ; Pfister, G.)
- Ideals, varieties, and algorithms : an introduction to computational algebraic geometry and commutative algebra (Cox, David A. et al.)

Complementarias

- Codificación de la información(Munuera Gómez, Juan - Tena Ayuso, Juan - Universidad de Valladolid)