FICHA IDENTIFICATIVA

Datos de la Asignatura

Código	44085
Nombre	Métodos algebraicos y sus aplicaciones
Ciclo	Máster
Créditos ECTS	3.0
Curso académico	2024 - 2025

Titulación(es)

Titulación	Centro	Curso	Periodo
2183 - M.U.Invest.Matemática	Facultad de Ciencias Matemáticas	1	Segundo cuatrimestre

Materias

Titulación	Materia	Carácter
2183 - M.U.Invest.Matemática	4 - Intensificación matemática fundamental	Optativa

RESUMEN

Objetivos de la asignatura

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.

Contextualización de la asignatura

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.

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 (RD 1393/2007) // RESULTADOS DEL APRENDIZAJE (RD 822/2021)

2183 - M.U.Invest.Matemática

- 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 (RD 1393/2007) // SIN CONTENIDO (RD 822/2021)

DESCRIPCIÓN DE CONTENIDOS

1. Aritmética modular y aplicaciones

1.1. Introducción al sistema de álgebra computacional GAP (Groups, Algorithms and Programming)
1.2. Conceptos básicos de aritmética modular.
1.3. Aplicaciones de la aritmética modular en criptografía y otros campos.
1.4. Reparto de secretos

2. Teoría de anillos y cuerpos. Aplicaciones

2.1. Revisión de los conceptos básicos de la Teoría de anillos y cuerpos.
2.2. Cuerpos finitos. Tratamiento con GAP.
2.3. Crisptografía basada en el problema del logaritmo discreto: ElGamal y criptografía elíptica. Firma digital. Tratamiento con el sistema computacional SageMath.
2.4. Factorización de números enteros y tests de primalidad

3. Introducción a la Teoría de códigos correctores de errores

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

4. Anillos de polinomios. Bases de Groebner y aplicaciones

4.1. Resultados básicos sobre anillos de polinomios de varias variables
4.2. Revisión de conceptos básicos de geometría algebraica.
4.3. Bases de Groebner.
4.4. Utilización del sistema de álgebra computacional GAP o Singular para el cálculo y manejo de las bases de Groebner.

5. 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

En cada sesión presencial, 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 en cinco actos de evaluación. Tres de ellos corresponden a tres entregas de trabajos académicos: dos portafolios sencillos en los que se resolverán problemas planteados por el profesor y relativos a los contenidos vistos en clase (con un peso del 15% cada uno) y la realización de un trabajo más amplio y elaborado que ampliará las aplicaciones y contenidos que se han trabajado (con un peso del 25%). Se realizará también un examen oral para valorar el conocimiento adquirido tanto en el portafolio como en el trabajo académico y la destreza del alumno en la comunicación oral (con un peso del 20%). Finalmente, se realizará a final de curso una prueba tipo test de los conceptos tratados a lo largo del curso (con un peso del 25%).

Si D=Defensa oral, E1 y E2=Estregas de problemas, F=Test Final y T=Trabajo final, la nota final de la asignatura es:

NotaFinal= 0.15*P1+0.15*P2+0.2*D+0.25*T+0.25*F.

Se considerará que el alumno ha superado la asignatura si NotaFinal>=5. Si algún alumno no supera la nota mínima citada anteriormente entonces podrá realizar un examen de recuperación final que corresponde al 70% de la asignatura. Si N es la nota obtenida en este examen de recuperación, entonces la nota final de la asignatura se calculará como

NotaFinal=0.15*P1+0.15*P2+0.7*N.

A los alumnos que tengan la dispensa de asistir a clase se les plantearán cuestiones sencillas de seguimiento y se les evaluará con los mismos criterios de evaluación que al resto de los estudiantes.

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)
- 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.)
- Codificación de la información (Munuera, Carlos; Tena, Juan)
- Coding and information theory (Roman, Steven)
- A first course in computational algebraic geometry / [electronic resource] (Decker, W.)
- Algebra for applications: cryptography, secret sharing, error-correcting, fingerprinting, compression (Slinko, Arkadii)