Guía docente de la asignatura

Teoría de Números y Criptografía

Fecha última actualización: 15/06/2021
Fecha de aprobación: 15/06/2021

Grado	Grado en Matemáticas	**Rama**	Ciencias
Módulo	Complementos de Álgebra	**Materia**	Teoría de Números y Criptografía

Curso	4º	**Semestre**	2º	**Créditos**	6	**Tipo**	Optativa

PRERREQUISITOS Y/O RECOMENDACIONES

Tener cursadas las asignaturas Álgebra I, II y III.

BREVE DESCRIPCIÓN DE CONTENIDOS (Según memoria de verificación del Grado)

- Introducción a la Teoría Algebraica de Números.
- Elementos enteros y descomposición de ideales en extensiones.
- Factorización y tests de primalidad.
- Criptografía asimétrica y criptosistemas.

COMPETENCIAS ASOCIADAS A MATERIA/ASIGNATURA

COMPETENCIAS GENERALES

- CG01 - Poseer los conocimientos básicos y matemáticos de las distintas materias que, partiendo de la base de la educación secundaria general, y apoyándose en libros de texto avanzados, se desarrollan en esta propuesta de título de Grado en Matemáticas
- CG02 - Saber aplicar esos conocimientos básicos y 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 de las Matemáticas y de los ámbitos en que se aplican directamente
- CG03 - Saber reunir e interpretar datos relevantes (normalmente de carácter matemático) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética
- CG04 - Poder transmitir información, ideas, problemas y sus soluciones, de forma escrita u oral, a un público tanto especializado como no especializado
- CG05 - Haber desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía
- CG06 - Utilizar herramientas de búsqueda de recursos bibliográficos

COMPETENCIAS ESPECÍFICAS

- CE01 - Comprender y utilizar el lenguaje matemático. Adquirir la capacidad de enunciar proposiciones en distintos campos de las matemáticas, para construir demostraciones y para transmitir los conocimientos matemáticos adquiridos
- CE02 - Conocer demostraciones rigurosas de teoremas clásicos en distintas áreas de Matemáticas
- CE03 - Asimilar la definición de un nuevo objeto matemático, en términos de otros ya conocidos, y ser capaz de utilizar este objeto en diferentes contextos
- CE04 - Saber abstraer las propiedades estructurales (de objetos matemáticos, de la realidad observada, y de otros ámbitos) y distinguirlas de aquellas puramente accidentales, y poder comprobarlas con demostraciones o refutarlas con contraejemplos, así como identificar errores en razonamientos incorrectos
- CE05 - Resolver problemas matemáticos, planificando su resolución en función de las herramientas disponibles y de las restricciones de tiempo y recursos
- CE06 - Proponer, analizar, validar e interpretar modelos de situaciones reales sencillas, utilizando las herramientas matemáticas más adecuadas a los fines que se persigan
- CE07 - Utilizar aplicaciones informáticas de análisis estadístico, cálculo numérico y simbólico, visualización gráfica, optimización u otras para experimentar en matemáticas y resolver problemas
- CE08 - Desarrollar programas que resuelvan problemas matemáticos utilizando para cada caso el entorno computacional adecuado

COMPETENCIAS TRANSVERSALES

- CT01 - Desarrollar cierta habilidad inicial de "emprendimiento" que facilite a los titulados, en el futuro, el autoempleo mediante la creación de empresas
- CT02 - Fomentar y garantizar el respeto a los Derechos Humanos y a los principios de accesibilidad universal, igualdad ante la ley, no discriminación y a los valores democráticos y de la cultura de la paz

RESULTADOS DE APRENDIZAJE (Objetivos)

- Conocer las dificultades de la factorización no solo de enteros sino también de números algebraicos.
- Conocer la extensión de factorizaciones a ideales.
- Calculo del grupo y el número de clase.
- Conocer las diferentes tecnologías de cifrado simétrico y las técnicas matemáticas en que se fundamentan.
- Conocer varios sistemas de cifrado asimétrico a partir de los problemas de teoría de números que los soportan.

PROGRAMA DE CONTENIDOS TEÓRICOS Y PRÁCTICOS

TEÓRICO

TEMARIO TEÓRICO:

- Tema 1. Introducción a la teoría algebraica de números. Números algebraicos.

- Tema 2. Tests y certificados de primalidad. Factorización.
- Tema 3. Fracciones continuas.
- Tema 4. Cuerpos cuadráticos y sucesiones de Lucas.
- Tema 5. Criptosistemas simétricos. Cifrados de bloque y flujo
- Tema 6. Criptosistema RSA.
- Tema 7. Criptosistemas basados en el logaritmo discreto.
- Tema 8. Curvas elípticas.
- Tema 9. Criptosistemas basados en curvas elípticas.

PRÁCTICO

BIBLIOGRAFÍA

BIBLIOGRAFÍA FUNDAMENTAL

- Neal Koblitz. A Course in Number Theory and Criptography. 2nd edition. Graduate Text in Mathematics, 114. Springer, 1994.
- I. Neven, H. S. Zuckerman and H. L. Montgomery. An introduction to the Theory of Numbers. John Wiley & Sons, 1991.
- Ian Stewart and David Tall. Algebraic Numer theory and Fermat's Last Theorem. A.K. Peters 2002.
- Hans Delfs and Helmut Knebl. Introduction to Cryptography. Principles and Applications. 3rd edition. Information Security and Cryptography. Springer, 2015.
- A. Enge. Elliptic curves and their applications to cryptography. An introduction. Kluwer Academic Publishers. 1999

BIBLIOGRAFÍA COMPLEMENTARIA

METODOLOGÍA DOCENTE

- MD01 Lección magistral/expositiva
- MD02 Sesiones de discusión y debate
- MD03 Resolución de problemas y estudio de casos prácticos
- MD04 Prácticas en sala de informática
- MD05 Seminarios
- MD06 Análisis de fuentes y documentos
- MD07 Realización de trabajos en grupo
- MD08 Realización de trabajos individuales

EVALUACIÓN (instrumentos de evaluación, criterios de evaluación y porcentaje sobre la calificación final)

EVALUACIÓN ORDINARIA

La evaluación de la asignatura en la convocatoria ordinaria se basará en las siguientes pruebas:

- Examen. El examen final de la asignatura será un examen escrito que comprenderá ejercicios relativos a los contenidos incluidos en el temario oficial. Este examen se realizará tanto en la convocatoria ordinaria como en las extraordinarias. Supondrá el 25% de la nota final
- Cuestionario. Un mínimo de 20 preguntas de opción múltiple. Supondrá el 15% de la nota final.
- Ejercicios. Relaciones de ejercicios personalizados que los alumnos deberán resolver y entregar a los profesores para su corrección. Se podrá pedir a los alumnos que defiendan presencialmente estos ejercicios. Estos ejercicios supondrán el 60% de la calificación final .

Aquellos alumnos que obtengan calificación suficiente con los ejercicios y cuestionario no tendrán que hacer el examen si no lo desean. La entrega de ejercicios y la realización del cuestionario sí son obligatorios.

EVALUACIÓN EXTRAORDINARIA

En la convocatoria extraordinaria se evaluará con el mismo método empleado en la evaluación ordinaria, dando un periodo extra a los alumnos para la entrega de los ejercicios personalizados.

EVALUACIÓN ÚNICA FINAL

Este modelo de evaluación consistirá en el cuestionario, que ponderará al 20%, el examen, que ponderará al 40%, junto con unos ejercicios personalizados, ponderables en un 40%, que serán propuestos en el examen y para los que los alumnos dispondrán de un máximo de dos días naturales.