Fecha de aprobación: **20/06/2022**

Guía docente de la asignatura

Teoría de Números y Criptografía (27011A4)

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:

Introducción a la teoría algebraica de números:

- Cuerpos finitos. Reciprocidad y formas cuadráticas, residuos cuadráticos.
- Cuadrados y suma de cuadrados.
- Fracciones continuas simples y regulares. La ecuación de Pell.
- Cuerpos de números cuadráticos y algunas ecuaciones diofánticas.
- Ecuaciones y curvas elípticas.
- Funciones aritméticas.
- Cuerpos de números algebraicos y sus ideales. La ecuación de Mordell.

Aplicación de la teoría elemental de números a la criptografía:

- Primalidad y factorización.
- Clave publica y criptosistemas RSA.
- Criptosistemas basados en el logaritmo discreto.
- 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. Niven, 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.
- H. Davenport. The higher arithmetic. An introduction to the theory of numbers. Eighth edition. Cambridge University Press. Cambridge, 2008.

BIBLIOGRAFÍA COMPLEMENTARIA

- Yu. I. Manin and A.A. Panchishkin. Introduction to modern number theory. Second edition. Encyclopaedia of mathematical Sciences, Vol. 49. Springer-Verlag, Berlin Heidelberg, 2005.

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

Con objeto de evaluar la adquisición de los contenidos y competencias a desarrollar se realizarán las siguientes pruebas evaluativas.

- Elaboración de un trabajo (en grupo) que será expuesto en las últimas semanas de clase. Esta actividad tendrá un valor del 30% de la nota final (15% la evaluación del trabajo y 15% la evaluación de la exposición). La asistencia a las exposiciones de los trabajos de todos los estudiantes estará incluida en la calificación de la exposición. La asistencia a clase no es obligatoria y por tanto no repercutirá en la calificación, salvo en el periodo de exposición de los trabajos.

- Prueba final escrita: la ponderación de esta actividad será del 70%.

Para aprobar la asignatura se deberá obtener al menos un 50% de la calificación máxima en cada uno de estos dos apartados.

EVALUACIÓN EXTRAORDINARIA

Consistirá en un examen escrito sobre los contenidos de la asignatura. A este examen tendrán que presentarse aquellos estudiantes que no hayan superado o no se hayan presentado a la convocatoria ordinaria, y todos aquellos que hayan solicitado evaluación única final.

La prueba de la convocatoria extraordinaria permitirá obtener el total de la calificación (no dependiendo necesariamente de la calificación del trabajo en grupo).

No obstante, aquellos estudiantes que hayan superado el trabajo en grupo y no hayan superado la prueba final escrita en convocatoria ordinaria, podrán optar a presentarse a la convocatoria extraordinaria, manteniendo la calificación del trabajo en grupo. En este caso, la nota final se calculará de igual forma que en la convocatoria ordinaria.

EVALUACIÓN ÚNICA FINAL

Los estudiantes que soliciten evaluación única final sólo tendrán que realizar una prueba escrita (la prueba final de la asignatura). En este escenario la calificación final será la obtenida en esta misma prueba.