GUIA DOCENTE DE LA ASIGNATURA

Teoría de Números y Criptografía

Curso 2016-17

Aprobada en Consejo de Departamento de fecha 5-9-2016

MÓDULO	MATERIA	CURSO	SEMESTRE	CRÉDITOS	TIPO
Complementos de Álgebra	Teoría de Números y Criptografía	4º	2º	6	Optativa

PROFESOR(ES)	DIRECCIÓN COMPLETA DE CONTACTO PARA TUTORÍAS (Dirección postal, teléfono, correo electrónico, etc.)
• Manuel Bullejos Lorenzo	Dpto. Álgebra, 2ª planta, Facultad de Ciencias. Despacho nº 38. Correo electrónico: bullejos@ugr.es
	HORARIO DE TUTORÍAS
	Consultar web http://www.ugr.es/~bullejos/ o http://algebra.ugr.es/

GRADO EN EL QUE SE IMPARTE	OTROS GRADOS A LOS QUE SE PODRÍA OFERTAR
Grado en Matemáticas	Física, Informática

PRERREQUISITOS Y/O RECOMENDACIONES (si procede)

Tener cursadas las asignaturas Álgebra I, II y III

BREVE DESCRIPCIÓN DE CONTENIDOS (SEGÚN MEMORIA DE VERIFICACIÓN DEL GRADO)

1.- Introducción a la Teoría Algebraica de Números.
2.- Criptografía asimétrica y criptosistemas.
3.- Factorización y tests de primalidad
4.- Elementos enteros y descomposición de ideales en anillos de enteros de cuerpos de números.

COMPETENCIAS GENERALES Y ESPECÍFICAS

CE1. 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.
. CE2. Conocer demostraciones rigurosas de algunos teoremas clásicos en distintas áreas de las Matemáticas.
. CE3. Asimilar la definición de un nuevo objeto matemático, en términos de otros ya conocidos, y ser capaz de utilizar este objeto en diferentes contextos.
. CE4. 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.
. CE5. Resolver problemas matemáticos, planificando su resolución en función de las herramientas disponibles y de las restricciones de tiempo y recursos.
. CE6. Proponer, analizar, validar e interpretar modelos de situaciones reales sencillas, utilizando las herramientas matemáticas más adecuadas a los fines que se persigan.
. CE7. Utilizar aplicaciones informáticas de análisis estadístico, cálculo numérico y simbólico, visualización gráfica, optimización u otras para experimentar en matemáticas y resolver problemas.
. CE8. Desarrollar programas que resuelvan problemas matemáticos utilizando para cada caso el entorno computacional adecuado.

OBJETIVOS (EXPRESADOS COMO RESULTADOS ESPERABLES DE LA ENSEÑANZA)

- Conocer las dificultades de la factorización no solo de enteros sino también de números algebráicos.
- Conocer la extensión de factorizaciones a ideales.
- Calculo del grupo y el número de clase.
- Conocer métodos de codificación y decodificación.

TEMARIO DETALLADO DE LA ASIGNATURA

TEMARIO TEÓRICO:

- Tema 1. Criptografía. Sistemas Criptográficos simétricos y asimétricos.
- Tema 2. Primalidad y Factorización.
- Tema 3. Números algebraicos.
- Tema 4. Extensiones Cuadráticas y Ciclotómicas.
- Tema 5. Factorización de enteros algebraicos.
- Tema 6. Factorización de ideales.
- Tema 7. Grupo y Número de Clase.

TEMARIO PRÁCTICO:
Prácticas de Laboratorio

Práctica 1. Codificación y decodificación de mensajes.
Práctica 2. Tests de Primalidad.
Práctica 3. Factorización en anillos de enteros cuadráticos.
Práctica 4. Unidades en anillos de enteros cuadráticos.
Práctica 5. Factorización de ideales.
Práctica 6. Cálculo de grupo de clase.

BIBLIOGRAFÍA

BIBLIOGRAFÍA FUNDAMENTAL:

- Neal Koblitz. A Course in Number Theory and Criptography. Graduate texts 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

ENLACES RECOMENDADOS

http://www.ugr.es/~algebra/ , http://www.ugr.es/~bullejos/

PROGRAMA DE ACTIVIDADES

	Actividades Presenciales				Actividades no Presenciales	
	Temas/Prácticas	Sesiones teóricas (horas)	Sesiones prácticas (horas)	Exámenes	Tutorías individuales (horas)	Trabajos individuales (horas)
Semana 1	T1	4	0		1	5
Semana 2	P1	0	4	1	1	5
Semana 3	T2	4	0		1	5
Semana 4	P2	0	4		1	5
Semana 5	T3	4	0		1	5
Semana 6	P3	0	4		1	5
Semana 7	T4	4	0		1	5
Semana 8	P4	0	4	1	1	5
Semana 9	T5	4	0		1	5
Semana 10	P5	0	4	1	1	5
Semana 11	T6	4	0		1	5
Semana 12	P6	0	4	1	1	5
Semana 13	T7	4	0		1	5
Semana 14	T8	4	0		1	5
Semana 15	P8	0	4	1	1	5
Total		32	28	5	15	75

METODOLOGÍA DOCENTE

La metodología docente a seguir en la materia (6 ECTS=150 h) constará de aproximadamente:

- Un 40% de docencia presencial en el aula (60 h.).
- Un 50% de estudio individualizado del alumno, búsqueda, consulta y tratamiento de información, resolución de problemas y casos prácticos, y realización de trabajos y exposiciones (75h.).
- Un 10% para tutorías individuales y/o colectivas y evaluación (15h).

Las actividades formativas se desarrollarán desde una metodología participativa y aplicada que se centra en el trabajo del estudiante (presencial y no presencial/individual y grupal). De entre las actividades formativas diseñadas para el grado (desarrolladas en el punto 5.1.) y encargadas de organizar los procesos de enseñanza y aprendizaje (lección magistral, actividades prácticas, seminarios o talleres, actividades individuales/grupales y las tutorías académicas), la materia desarrollará aquéllas actividades que más se adecuen a los contenidos y competencias a adquirir por el alumnado.

EVALUACIÓN (INSTRUMENTOS DE EVALUACIÓN, CRITERIOS DE EVALUACIÓN Y PORCENTAJE SOBRE LA CALIFICACIÓN FINAL, ETC.)

Como Normativa General, todo lo que sigue ha de regirse por la "Normativa de Evaluación y Calificación de los estudiantes de la Universidad de Granada" aprobada por Consejo de Gobierno en su sesión extraordinaria de 20 de Mayo de 2013. Con objeto de evaluar la adquisición de los contenidos y competencias a desarrollar en la materia, se utilizará un sistema de evaluación diversificado, seleccionando las técnicas de evaluación más adecuadas para la asignatura en cada momento, que permita poner de manifiesto los diferentes conocimientos y capacidades adquiridos por el alumnado al cursar la asignatura. De entre las siguientes técnicas evaluativas se utilizarán alguna o algunas de ellas:

- Prueba escrita: exámenes de ensayo, pruebas objetivas, resolución de problemas, casos o supuestos, pruebas de respuesta breve, informes y diarios de clase. De este tipo de pruebas de evaluación se realizarán concretamente cinco a lo largo del curso y todas ellas contrastarán conocimientos teóricos y prácticos.
- Prácticas de ordenador: A lo largo del curso se realizarán siete prácticas de ordenador en las que se abordará la resolución de diversos problemas usando adecuados paquetes informáticos. La realización de dichas prácticas es obligatoria y la no asistencia a alguna de las sesiones programadas habrá de ser justificada.
- Prueba oral: exposiciones de trabajos orales en clase, individuales o en grupo, sobre contenidos de la asignatura (seminario) y sobre ejecución de tareas prácticas correspondientes a competencias concretas.
- Observación: escalas de observación, en donde se registran conductas que realiza el alumno en la ejecución de tareas o actividades que se correspondan con las competencias.
- Técnicas basadas en la asistencia y participación activa del alumno en clase, seminarios y tutorías: trabajos en grupos reducidos sobre supuestos prácticos propuestos.

Aquellos alumno(a)s que no puedan seguir este proceso de evaluación continua y, en orden a que puedan acreditar las competencias exigidas en esta Guía Docente, podrán realizar en la convocatoria ordinaria una **evaluación única final** de acuerdo con la normativa general aludida al principio. En la convocatoria extraordinaria podrán concurrir todos los estudiantes con independencia de haber seguido o no un proceso de evaluación continua. El sistema de calificaciones se expresará mediante calificación numérica de acuerdo con lo establecido en el artículo 5 del R. D 1125/2003, de 5 de septiembre, por el que se establece el sistema europeo de créditos y el sistema de calificaciones en las titulaciones universitarias de carácter oficial y validez en el territorio nacional. La calificación final corresponderá a la puntuación ponderada de los diferentes aspectos y actividades que integran el sistema de evaluación teniendo las dos pruebas

escritas programadas el mayor peso (al menos del 85%) sobre la calificación total mientras que las Prácticas de ordenador y otras técnicas aplicadas lo tendrán del restante 15%.
INFORMACIÓN ADICIONAL
Cumplimentar con el texto correspondiente en cada caso.