TEORÍA DE NÚMEROS Y CRIPTOGRAFÍA
GUÍA DOCENTE CURSO 2018-19

Titulación:	Grado en Matemáticas				**701G**
Asignatura:	Teoría de números y criptografía				**419**
Materia:	Teoría de números y criptografía				
Módulo:	Optativas				
Modalidad de enseñanza de la titulación:	Presencial		**Carácter:**	Optativa	
Curso:	4	**Créditos ECTS:** 6,00	**Duración:**	Semestral	
Horas presenciales:	60,00		**Horas estimadas de trabajo autónomo:**	90,00	

Idiomas en que se imparte la asignatura:	Español
Idiomas del material de lectura o audiovisual:	Español

DEPARTAMENTOS RESPONSABLES DE LA DOCENCIA

MATEMÁTICAS Y COMPUTACIÓN					**R111**
Dirección:	C/ Madre de Dios, 53			**Código postal:**	26006
Localidad:	Logroño		**Provincia:**	La Rioja	
Teléfono:	941299452	**Fax:** 941299460	**Correo electrónico:**	dpto.dmc@unirioja.es	

PROFESORADO PREVISTO

Profesor:	Varona Malumbres, Juan Luis			**Responsable de la asignatura**	
Teléfono:	941299451	**Correo electrónico:**	jvarona@unirioja.es		
Despacho:	3206	**Edificio:**	CENTRO CIENTÍFICO TECNOLÓGICO	**Tutorías:**	Consultar

DESCRIPCIÓN DE LOS CONTENIDOS

- Aproximación de un número real por racionales, fracciones continuas. Irracionalidad y trascendencia.
- Congruencias lineales y no lineales, residuos cuadráticos. Ecuaciones diofánticas.
- Funciones aritméticas y multiplicativas.
- Distribución de números primos.
- Aproximación de Kummer al último Teorema de Fermat.
- Criptografía clásica. El sistema RSA y la factorización. Otros criptosistemas de clave pública. Sistemas con firma. Funciones de una dirección. Distribución de claves y acuerdo de claves. Criptografía asimétrica.

REQUISITOS PREVIOS DE CONOCIMIENTOS Y COMPETENCIAS PARA PODER CURSAR CON ÉXITO LA ASIGNATURA

Ninguno especificado.

CONTEXTO

Ésta es una preciosa asignatura dentro del Grado en Matemáticas. Aunque es una asignatura optativa (y, de hecho, no existe en los planes de estudio de muchas titulaciones de matemáticas, algo achacable únicamente a las estúpidas luchas entre áreas de conocimiento oficialmente reconocidas), es una pena que cualquier matemático se pierda el tipo de conocimientos que en una asignatura como esta se imparten.
Por una parte, en la asignatura se aborda la teoría de números, que ha sido uno de los motores principales de las matemáticas durante más de dos milenios. Por otra parte, también se estudia criptografía, una moderna aplicación de la teoría de números que es causa de que, en el contexto del mundo tecnológico actual, la teoría de números tenga una importancia práctica indiscutible.

COMPETENCIAS

Competencias generales

CG 1. Comprender el lenguaje matemático, enunciados y demostraciones, identificando razonamientos incorrectos, y utilizarlo en diversos problemas y aplicaciones.
CG 2. Asimilar la definición de un nuevo objeto matemático, en términos de otros ya conocidos, y ser capaz de utilizar este objeto en diferentes contextos.
CG 3. Disponer de una perspectiva histórica del desarrollo de la Matemática y conocer demostraciones rigurosas de algunos teoremas clásicos.

CG 4. Adquirir la capacidad para enunciar proposiciones en distintos campos de la Matemática, para construir demostraciones y para transmitir el conocimiento matemático adquirido.
CG 5. Saber abstraer las propiedades estructurales de objetos matemáticos y poder comprobarlas con demostraciones o refutarlas con contraejemplos.
CG 6. Relacionar el conocimiento especializado de Matemáticas con el conocimiento general en el que se inserta y con las herramientas que utiliza cuando se aplica en diversas opciones profesionales, especialmente en el marco de las TIC.
CG 7. Saber abstraer las propiedades estructurales de objetos de la realidad observada y de otros ámbitos, distinguiéndolas de aquellas puramente ocasionales, comprobando la aplicabilidad de las Matemáticas.
CG 8. Capacitar para el aprendizaje autónomo de nuevos conocimientos y técnicas.

Competencias específicas

CE 1. Resolver problemas de Matemáticas, mediante habilidades de cálculo básico y otras técnicas, planificando su resolución en función de las herramientas de que se disponga y de las restricciones de tiempo y recursos.
CE 2. Utilizar aplicaciones informáticas de análisis estadístico, cálculo numérico y simbólico, visualización gráfica, optimización, u otras, para experimentar en Matemáticas y resolver problemas.
CE 3. Proponer, analizar, validar e interpretar modelos de situaciones reales sencillas, utilizando las herramientas matemáticas más adecuadas a los fines que se persigan.
CE 4. Encontrar soluciones algorítmicas de problemas matemáticos y de aplicación (de ámbito académico, técnico, financiero o social), sabiendo comparar distintas alternativas, según criterios de adecuación, complejidad y coste.
CE 9. Habilidades para comunicar las Matemática, sus ideas, problemas y métodos, a públicos con diverso grado de especialización.

RESULTADOS DEL APRENDIZAJE

- Comprender distintos aspectos de la teoría de números analítica y algebraica, así como sus aplicaciones para resolver diferentes problemas en matemáticas.
- Conocer las aplicaciones de la teoría de números en la transmisión de información de manera segura. Entender el desarrollo de la criptografía desde sus comienzos hasta ahora, y los diversos objetivos alcanzados y problemas que surgen.

TEMARIO

1. Aritmética básica
2. Algunas ecuaciones diofánticas
3. Congruencias
4. Criptografía
5. Fracciones continuas
6. Irracionalidad y trascendencia

BIBLIOGRAFÍA

Tipo:	Título
Básica	J. L. Varona, Recorridos por la Teoría de Números, Electolibris y Real Sociedad Matemática Española, Murcia, 2014.
Complementaria	E. Aparicio, Teoría de los números, Servicio Editorial de la Universidad del País Vasco, Bilbao, 1993.
Complementaria	T. M. Apostol, Introducción a la teoría analítica de números, Reverté, 1980.
Complementaria	J. Cilleruelo y A. Córdoba, La teoría de los números, Biblioteca Mondadori, Madrid, 1992.
Complementaria	G. H. Hardy y E. M. Wright, An introduction to the theory of numbers, 5.ª ed., Oxford University Press, 1979.
Complementaria	Hua Loo Keng, Introduction to number theory, Springer-Verlag, 1982.
Complementaria	J. M. De Koninck y F. Luca, Analytic Number Theory: Exploring the Anatomy of Integers, American Mathematical Society, 2012
Complementaria	M. B. Nathanson, Elementary methods in number theory, Springer, 2000.
Complementaria	I. Niven, H. S. Zuckerman y H. L. Montgomery, An introduction to the theory of numbers, 5.ª ed., Wiley, 1991.
Complementaria	H. E. Rose, A course in number theory, 2.ª ed., Oxford University Press, 1996.
Complementaria	A. B. Shidlovskii, Aproximaciones diofánticas y números trascendentes, Servicio Editorial de la Universidad del País Vasco, Bilbao, 1989.

Recursos en Internet
Libro de texto para la asignatura http://www.unirioja.es/cu/jvarona/libroTN.html
Buscador

http://www.google.com/

Descripción del método de evaluación
http://www.mat.uab.cat/matmat/PDFv2011/v2011n06.pdf

METODOLOGÍA

Modalidades organizativas

Clases teóricas
Seminarios y talleres
Clases prácticas
Estudio y trabajo autónomo individual

Métodos de enseñanza

Método expositivo - Lección magistral
Estudio de casos
Resolución de ejercicios y problemas
Aprendizaje orientado a proyectos
Aprendizaje cooperativo

ORGANIZACIÓN

Actividades presenciales	Tamaño de grupo	Horas
Clases prácticas de aula	Reducido	15,00
Clases prácticas de laboratorio o aula informática	Informática	5,00
Clases teóricas	Grande	40,00
Total de horas presenciales		60,00

Trabajo autónomo del estudiante	Horas
Estudio autónomo individual o en grupo	45,00
Resolución individual de ejercicios, cuestiones u otros trabajos, actidades en biblioteca o similar	45,00
Total de horas de trabajo autónomo	90,00

Total de horas	150,00

EVALUACIÓN

Sistemas de evaluación	Recuperable	No Recup.
Pruebas escritas	50%	
Pruebas de ejecución de tareas reales y/o simuladas	50%	
Total	100%	

Comentarios

A cada alumno se le propondrán varios problemas para resolver de manera individual. Exponiendo las soluciones en clase (evaluación continua que en este formulario aparece descrita como "Pruebas de ejecución de tareas reales y/o simulada"), se podrá sacar un 5. Para obtener más nota, habrá que acudir al examen final, que no es obligatorio.
La nota final de la asignatura se calculará como sigue:

- Sea x la nota al exponer sus problemas resueltos (con x entre 0 y 5).
- Sea y la nota del examen final (con y entre 0 y 10).
- La nota final será $N(x,y) = x + (1-x/10)y$

Obsérvese que $N(5,y)$ es superior a 5 para todo y (incluido y=0), luego el examen final no es obligatorio.
Además $N(x,10) = 10$ para cualquier x, luego incluso renunciando a la evaluación continua se puede obtener un 10 en la asignatura.
A los alumnos a tiempo parcial que no acudan a clase se les evaluará con la misma fórmula $N(x,y)$ con x=0.

Criterios críticos para superar la asignatura

A cada alumno se le propondrán varios problemas para resover de manera individual. Exponiendo las soluciones en clase, se podrá sacar un 5. Para obtener más nota, habrá que acudir al examen final, que no es obligatorio.
El criterio crítico para superar la asignatura es obtener, como nota final $N(x,y)$, al menos un 5.