GUIA DOCENTE DE LA ASIGNATURA (∞)

TEORÍA DE NÚMEROS Y CRIPTOGRAFÍA

Curso 2020-2021

(Fecha última actualización: 10/07/2020)

(Fecha de aprobación en Consejo de Departamento: 14/07/2020)

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

PROFESORES[1]	DIRECCIÓN COMPLETA DE CONTACTO PARA TUTORÍAS (Dirección postal, teléfono, correo electrónico, etc.)
• Enrique Aznar García: Parte I "Teoría de Números" • Fco. Javier Lobillo Borrero: Parte II "Curvas Elípticas y Criptografía"	E. Aznar: Dpto. de Álgebra, Sección de Matemáticas, Facultad de Ciencias. Despacho nº 30, 2ª planta. Correo electrónico: eaznar@ugr.es F. J. Lobillo: Dpto. de Álgebra, ETSIIT, 2ª planta, Despacho nº 13. Dpto. de Álgebra, Sección de Matemáticas. Facultad de Ciencias. Despacho 0.3 Correo electrónico: jlobillo@ugr.es
	HORARIO DE TUTORÍAS Y/O ENLACE A LA PÁGINA WEB DONDE PUEDAN CONSULTARSE LOS HORARIOS DE TUTORÍAS[1]
	Consultar en http://algebra.ugr.es

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

PRERREQUISITOS Y/O RECOMENDACIONES (si procede)
Tener cursadas las asignaturas Álgebra I, II y III.

[1] Consulte posible actualización en Acceso Identificado > Aplicaciones > Ordenación Docente

(∞) Esta guía docente debe ser cumplimentada siguiendo la "Normativa de Evaluación y de Calificación de los estudiantes de la Universidad de Granada" (http://secretariageneral.ugr.es/pages/normativa/fichasugr/ncg7121/!)

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 GENERALES Y ESPECÍFICAS

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.
CB1 - Que los estudiantes hayan demostrado poseer y comprender conocimientos en un área de estudio que parte de la base de la educación secundaria general, y se suele encontrar a un nivel que, si bien se apoya en libros de texto avanzados, incluye también algunos aspectos que implican conocimientos procedentes de la vanguardia de su campo de estudio.
CB2 - Que los estudiantes sepan aplicar sus conocimientos a su trabajo o vocación de una forma profesional y posean las competencias que suelen demostrarse por medio de la elaboración y defensa de argumentos y la resolución de problemas dentro de su área de estudio.
CB3 - Que los estudiantes tengan la capacidad de reunir e interpretar datos relevantes (normalmente dentro de su área de estudio) para emitir juicios que incluyan una reflexión sobre temas relevantes de índole social, científica o ética.
CB4 - Que los estudiantes puedan transmitir información, ideas, problemas y soluciones a un público tanto especializado como no especializado.
CB5 - Que los estudiantes hayan desarrollado aquellas habilidades de aprendizaje necesarias para emprender estudios posteriores con un alto grado de autonomía.
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.

OBJETIVOS (EXPRESADOS COMO RESULTADOS ESPERABLES DE LA ENSEÑANZA)

- 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.

TEMARIO DETALLADO DE LA ASIGNATURA

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. Curvas elípticas.
Tema 6. Criptosistemas simétricos. Cifrados de bloque y flujo
Tema 7. Criptosistema RSA.
Tema 8. Criptosistemas basados en el logaritmo discreto.
Tema 9. Criptosistemas basados en curvas elípticas.

BIBLIOGRAFÍA

- 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.

ENLACES RECOMENDADOS

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.)

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. En las convocatorias extraordinarias se evaluará con el mismo método, dando un periodo extra a los alumnos para la entrega de los ejercicios personalizados.

El sistema de calificaciones se expresará mediante calificación numérica de acuerdo con lo establecido en el art. 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. Todo lo relativo a la evaluación se regirá por la Normativa de evaluación y calificación de los estudiantes vigente en la Universidad de Granada, que puede consultarse en: Normativa de Evaluación y Calificación de los Estudiantes de la UGR.

DESCRIPCIÓN DE LAS PRUEBAS QUE FORMARÁN PARTE DE LA EVALUACIÓN ÚNICA FINAL ESTABLECIDA EN LA “NORMATIVA DE EVALUACIÓN Y DE CALIFICACIÓN DE LOS ESTUDIANTES DE LA UNIVERSIDAD DE GRANADA”

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.

ESCENARIO A (ENSEÑANZA-APRENDIZAJE PRESENCIAL Y NO PRESENCIAL)

ATENCIÓN TUTORIAL

HORARIO (Según lo establecido en el POD)	HERRAMIENTAS PARA LA ATENCIÓN TUTORIAL (Indicar medios telemáticos para la atención tutorial)
El horario de tutorías se puede consultar en http://algebra.ugr.es Para evitar aglomeraciones o el consumo innecesario de recursos informáticos, los alumnos deberán solicitar cita previa mediante las herramientas asíncronas detalladas a continuación.	Además de la atención presencial si las medidas sanitarias lo permiten, se emplearán los siguientes medios telemáticos: • Correo electrónico • Sesiones de Google Meet (Síncrono) • Mensajes en las plataformas docentes • Canal de Telegram (Prof. Lobillo) Las herramientas aquí descritas podrán ser sustituidas por cualquier otra equivalente que la UGR ponga a disposición de sus miembros.

MEDIDAS DE ADAPTACIÓN DE LA METODOLOGÍA DOCENTE

- Las clases serán emitidas en directo mediante Google Meet o sistema equivalente proporcionado por la Universidad.
- Se potenciará el uso de herramientas de cálculo simbólico para la resolución de ejercicios, ya que es más conveniente el uso de herramientas CAS como Sagemath para la resolución de ejercicios en línea.

MEDIDAS DE ADAPTACIÓN DE LA EVALUACIÓN (Instrumentos, criterios y porcentajes sobre la calificación final)

Convocatoria Ordinaria

- **Entrega de ejercicios.** En cada tema los alumnos deberán entregar resueltos ejercicios propuestos, muchos de ellos personalizados, a través de PRADO o plataforma equivalente. En la evaluación de cada ejercicio se tendrá en cuenta la precisión y corrección de los razonamientos. Los ejercicios supondrán el 60% de la nota final.
- **Cuestionario online.** Cuestionario de un mínimo de 20 preguntas con opción múltiple de respuesta. Los fallos podrán restar de forma proporcional al número de opciones. El cuestionario supondrá el 15% de la nota final.
- **Examen.** Examen teórico-práctico de entre dos y tres horas de duración. Este examen se celebrará de forma presencial. En la evaluación de cada pregunta se tendrá en cuenta la precisión y corrección de los razonamientos. El examen supondrá el 25% de la nota final.

Convocatoria Extraordinaria

Se empleará el mismo método que en la evaluación ordinaria, fijando nuevas fechas de entrega de los ejercicios propuestos.

Evaluación Única Final

Este modelo de evaluación consistirá en el cuestionario, que ponderará al 20%, el examen, que ponderará al 40%, ambos realizados de idéntica forma a las convocatorias anteriores, junto con unos ejercicios personalizados, ponderables en un 40%, que serán propuestos al finalizar el

examen y para los que los alumnos dispondrán de un máximo de dos días naturales, y entregados a través de las plataformas empleadas.

ESCENARIO B (SUSPENSIÓN DE LA ACTIVIDAD PRESENCIAL)

ATENCIÓN TUTORIAL

HORARIO (Según lo establecido en el POD)	HERRAMIENTAS PARA LA ATENCIÓN TUTORIAL (Indicar medios telemáticos para la atención tutorial)
El horario de tutorías se puede consultar en http://algebra.ugr.es Para evitar el consumo innecesario de recursos informáticos, los alumnos deberán solicitar cita previa mediante correo electrónico, mensaje a través de las plataformas docentes, o mensaje en el canal de Telegram (Prof. Lobillo) de la asignatura.	Se emplearán los siguientes medios telemáticos: • Correo electrónico • Sesiones de Google Meet (Síncrono) • Mensajes en plataformas docentes • Canal de Telegram (Prof. Lobillo) Las herramientas aquí descritas podrán ser sustituidas por cualquier otra equivalente que la UGR ponga a disposición de sus miembros.

MEDIDAS DE ADAPTACIÓN DE LA METODOLOGÍA DOCENTE

- Las clases serán emitidas en directo mediante Google Meet o sistema equivalente propuesto por la UGR.
- Se potenciará el uso de herramientas de cálculo simbólico para la resolución de ejercicios, ya que es más conveniente el uso de herramientas CAS como Sagemath para la resolución de ejercicios en línea.

MEDIDAS DE ADAPTACIÓN DE LA EVALUACIÓN (Instrumentos, criterios y porcentajes sobre la calificación final)

Convocatoria Ordinaria

- **Entrega de ejercicios.** En cada tema los alumnos deberán entregar resueltos ejercicios propuestos, muchos de ellos personalizados, a través de PRADO o plataforma equivalente. En la evaluación de cada ejercicio se tendrá en cuenta la precisión y corrección de los razonamientos. Los ejercicios supondrán el 60% de la nota final.
- **Cuestionario online.** Cuestionario de un mínimo de 20 preguntas con opción múltiple de respuesta. Los fallos podrán restar de forma proporcional al número de opciones. El cuestionario supondrá el 15% de la nota final.
- **Examen.** Examen teórico-práctico de entre dos y tres horas de duración. El enunciado del examen, que podrá contener ejercicios personalizados, se publicará en PRADO en la hora acordada, y los alumnos dispondrán del tiempo indicado para subir la resolución del mismo. En la evaluación de cada pregunta se tendrá en cuenta la precisión y corrección de los razonamientos. Durante la corrección se podrá solicitar a aquellos alumnos que los profesores estimen oportuno, una conexión síncrona mediante Google Meet, plataforma equivalente o teléfono para explicar la respuesta a las preguntas planteadas. El examen

supondrá el 25% de la nota final.
Convocatoria Extraordinaria
Se empleará el mismo método que en la evaluación ordinaria, fijando nuevas fechas de entrega de los ejercicios propuestos.
Evaluación Única Final
Este modelo de evaluación consistirá en el cuestionario, que ponderará al 20%, el examen, que ponderará al 40%, ambos realizados de idéntica forma a las convocatorias anteriores, junto con unos ejercicios personalizados, ponderables en un 40%, que serán propuestos al finalizar el examen y para los que los alumnos dispondrán de un máximo de dos días naturales, y entregados a través de las plataformas empleadas.