1. Identificación

1.1. De la Asignatura

Curso Académico	2023/2024
Titulación	MÁSTER UNIVERSITARIO EN MATEMÁTICA AVANZADA
Nombre de la Asignatura	TEORÍA DE NÚMEROS
Código	6362
Curso	PRIMERO y PRIMERO(IC)
Carácter	OPTATIVA
N.º Grupos	2
Créditos ECTS	6
Estimación del volumen de trabajo del alumno	150
Organización Temporal/Temporalidad	Cuatrimestre
Idiomas en que se imparte	INGLÉS : Grupo 1 ESPAÑOL : Grupo 1,Y(IC)

1.2. Del profesorado: Equipo Docente

Coordinación de la asignatura JOSE JOAQUIN BERNAL BUITRAGO	Área/Departamento	ÁLGEBRA/MATEMÁTICAS
	Categoría	PROFESOR PERMANENTE LABORAL
	Correo Electrónico / Página web / Tutoría electrónica	josejoaquin.bernal@um.es Tutoría Electrónica: SÍ

Grupo de Docencia: 1 y Y Coordinación de los grupos:1 y Y(IC)	Teléfono, Horario y Lugar de atención al alumnado	Duración	Día	Horario	Lugar
		Anual	Lunes	13:00- 15:00	(Sin Extensión), Facultad de Matemáticas y Aulario General B1.1.007
		Anual	Martes	13:00- 14:00	(Sin Extensión), Facultad de Matemáticas y Aulario General B1.1.007
		Anual	Miércoles	13:00- 14:00	(Sin Extensión), Facultad de Matemáticas y Aulario General B1.1.007
		Anual	Jueves	13:00- 14:00	(Sin Extensión), Facultad de Matemáticas y Aulario General B1.1.007
		Anual	Viernes	13:00- 14:00	(Sin Extensión), Facultad de Matemáticas y Aulario General B1.1.007

2. Presentación

En esta asignatura, partiendo de los conocimientos algebraicos adquiridos en cursos anteriores, se realizará una introducción a algunos de los métodos de la teoría elemental de números y sus aplicaciones, en paricular al campo de la Criptología.

3. Condiciones de acceso a la asignatura

3.1 Incompatibilidades

No consta

3.2 Recomendaciones

Las propias del Máster de Matemática Avanzada. No obstante, se espera que el alumno esté familiarizado con los fundamentos del álgebra lineal y las estructuras algebraicas. A título indicativo, entendemos por contenidos básicos algunos de los tratados en las siguientes asignaturas del plan de estudios del Grado en Matemáticas de la Universidad de Murcia "Álgebra Lineal", "Ampliación de Álgebra Lineal y Geometría", "Grupos y Anillos" y "Ecuaciones Algebraicas".

4. Competencias

4.1 Competencias Básicas

· CB6. Poseer y comprender conocimientos que aporten una base u oportunidad de ser originales en el desarrollo y/o aplicación de ideas, a menudo en un contexto de investigación

· CB7. Que los estudiantes sepan aplicar los conocimientos adquiridos y su capacidad de resolución de problemas en entornos nuevos o poco conocidos dentro de contextos más amplios (o multidisciplinares) relacionados con su área de estudio

· CB8. Que los estudiantes sean capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios a partir de una información que, siendo incompleta o limitada, incluya reflexiones sobre las responsabilidades sociales y éticas vinculadas a la aplicación de sus conocimientos y juicios

· CB9. Que los estudiantes sepan comunicar sus conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades

· CB10. Que los estudiantes posean las habilidades de aprendizaje que les permitan continuar estudiando de un modo que habrá de ser en gran medida autodirigido o autónomo.

4.2 Competencias de la titulación

· CG2. Ser capaz de aplicar técnicas matemáticas en diversas actividades profesionales.
· CG3. Ser capaz de aplicar técnicas matemáticas en el desarrollo de proyectos de I+D+i.
· CG1. Ser capaz de aplicar técnicas matemáticas de investigación en diversos campos, tanto de matemática fundamental como aplicada.
· CG4. Ser capaz de aplicar los conocimientos adquiridos para resolver problemas en entornos nuevos o poco conocidos tanto en matemáticas como en contextos más generales o multidisciplinares que estén relacionados con su especialidad. (Meces/BOE (a)).
· CG5. Ser capaces de integrar conocimientos y enfrentarse a la complejidad de formular juicios y conjeturas a partir de información incompleta o limitada en la aplicación de técnicas y conocimientos matemáticos. (Meces/BOE (b)).
· CG6. Saber comunicar conclusiones y los conocimientos y razones últimas que las sustentan a públicos especializados y no especializados de un modo claro y sin ambigüedades. (Meces/BOE (c))
· CG7. Poseer habilidades de aprendizaje que permitan continuar futuros estudios de forma autodirigido o autónoma. (Meces/BOE (d))
· CG8. Ser capaz de trabajar en grupo y en equipos multidisciplinares.
· CE1. Poseer conocimientos teóricos y prácticos de un área de conocimiento de matemáticas para poder acceder a los estudios de doctorado y realizar una tesis doctoral.
· CE2. Ser capaz de leer críticamente trabajos especializados o de investigación e incorporar los resultados a su trabajo.
· CE3. Ser capaz de abstraer y analizar información sobre diversos procedimientos, y de realizar razonamientos lógicos e identificar errores.
· CE4. Ser capaz de realizar transferencia de resultados matemáticos a otras disciplinas y actividades.
· CE5. Ser capaz de modelar matemáticamente problemas teóricos o reales.
· CE6. Conocer técnicas de resolución y ser capaz de idear procedimientos de resolución de los modelos matemáticos objetos de estudio.
· CE7. Manejar las herramientas informáticas que sirven de ayuda a la resolución de los problemas objeto de estudio.

4.3 Competencias transversales y de materia

5. Contenidos

Bloque 1: TEORÍA ELEMENTAL DE NÚMEROS

TEMA 1. Factorización única. Aplicaciones.

Factorización en dominios de ideales principales. Factorización en Z y en k[x].

TEMA 2. Congruencias en Z.

El Teorema chino de los restos. La estructura de U(Z/nZ). El pequeño Teorema de Fermat. El Teorema de Wilson.

TEMA 3. Funciones aritméticas.

Suma y número de divisores. Fórmula de inversión de Moebius.

TEMA 4. Generalización de Euler del Teorema de Fermat.

Función phi de Euler. Teorema de Euler.

TEMA 5. Raíces primitivas e índices.

Orden de un entero módulo n. Raíces primitivas módulo un número primo.

Bloque 2: CRIPTOLOGÍA

TEMA 1. Introducción a la Criptología.

Criptosistemas simétricos o de clave privada. Criptosistemas asimétricos o de clave pública.

6. Metodología Docente

Actividad Formativa	Metodología	Horas Presenciales	Trabajo Autónomo	Volumen de trabajo
Clases de exposición teórica	AF1: En las clases de teoría se introducirán los conceptos, ejemplos y problemas básicos correspondientes a la asignatura. Se utilizará principalmente la lección magistral impartida por el profesor, intercalada en ocasiones con discusiones que estimulen la participación de los alumnos. Para los alumnos en modalidad semipresencial se proporcionará bibliografía en la que podrán estudiar los contenidos desarrollados en clase.	35	40	75.00

Actividad Formativa	Metodología	Horas Presenciales	Trabajo Autónomo	Volumen de trabajo
Exposición de trabajos	AF3: Todos los alumnos tendrán que preparar una parte del contenido teórico de la asignatura o un tema de ampliación que deberán exponer al resto de compañeros y al profesor. La asignación de esos contenidos se hará con suficiente antelación.	8	16	24.00
Tutorías individuales y en grupos reducidos	AF4: Serán utilizadas para resolver de forma individual, o en pequeños grupos, con el profesor aquellas dudas o dificultades que los alumnos puedan encontrar en el estudio de la materia y la resolución de los problemas planteados.	5		5
Resolución de problemas	AF2: Resolución de problemas de forma autónoma por los alumnos.	0	46	46.00
	Total	48	102	150

7. Horario de la asignatura

https://www.um.es/web/estudios/masteres/matematica-avanzada/2023-24#horarios

8. Sistema de Evaluación

Métodos / Instrumentos	SE1: Resolución de problemas/Casos prácticos: Los profesores propondrán problemas/casos prácticos para que sean resueltos por los alumnos (individualmente o en grupo) explicando las soluciones de forma oral y/o escrita.
Criterios de Valoración	A lo largo del curso el profesor indicará a los alumnos la resolución de algunos problemas y propondrá otros tantos para que cada alumno elija un mínimo número de ellos. El alumno deberá mostrar autonomía seleccionando por su cuenta los problemas entre estos últimos. Con la resolución de todos estos problemas el alumno elaborará un dossier del trabajo realizado durante el desarrollo de la asignatura que será entregado al profesor al final del periodo lectivo para su valoración. Cada uno de los alumnos será citado individualmente para responder preguntas del profesor sobre el dossier presentado (SE7). Para la valoración del trabajo se tendrán en cuenta la selección de los problemas resueltos, el planteamiento de las soluciones, la correcta utilización de los conceptos y herramientas matemáticos utilizados, la correción, rigor y claridad de la explicación de las soluciones y su interpretación.
Ponderación	55
Métodos / Instrumentos	SE2: Exposición y realización de trabajos: Realización de trabajos, informes y exposición de los resultados obtenidos y los procedimientos usados, así como respuestas razonadas a las posibles cuestiones que se plantee sobre el mismo.
Criterios de Valoración	Todos los alumnos deberán realizar una exposición al profesor y al resto de los alumnos, de una parte de la asignatura que será asignada a cada uno de ellos por el profesor. Durante la exposición el alumno deberá responder a las preguntas planteadas por el profesor y el resto de alumnos. Para su valoración se tendrá en cuenta la corrección, rigor y claridad en la exposición, la correcta utilización de los conceptos y herramientas matemáticos utilizados, la interpretación de los conceptos y resultados expuestos y la aportación personal del alumno en la organización de la materia expuesta.
Ponderación	25

Métodos / Instrumentos	SE3: Pruebas escritas (exámenes): Pruebas objetivas, de desarrollo, de respuesta corta, de ejecución de tareas, de escala de actitudes realizadas por los alumnos para mostrar los conocimientos teóricos y prácticos adquiridos.
Criterios de Valoración	No se utilizará este método de evaluación.
Ponderación	0
Métodos / Instrumentos	SE4: Trabajos del alumno: Trabajos escritos con independencia de que se realicen individual o grupalmente.
Criterios de Valoración	El alumno que lo desee puede añadir a su dossier trabajos escritos de ampliación de la materia explicada durante el curso. Esta parte es opcional y compensatoria de la resolución de problemas y se añadirá al dossier mencionado en (SE1). Para su valoración se tendrá en cuenta la corrección, rigor y claridad en la exposición, la correcta utilización de los conceptos y herramientas matemáticos utilizados, la interpretación de los conceptos y resultados expuestos y la aportación personal del alumno en la organización de la materia expuesta.
Ponderación	0
Métodos / Instrumentos	SE5: Asistencia y participación en clase: Registros de participación, de realización de actividades, cumplimiento de plazos, participación en clase, asistencia a clases y prácticas
Criterios de Valoración	Se tendrá en cuenta la participación activa en clase y, en especial, la asistencia y participación en las sesiones de exposición. (ver Observaciones)
Ponderación	10
Métodos / Instrumentos	SE6: Examen práctico: Actividades prácticas y/o de laboratorio de computadores para mostrar el conocimiento adquirido en la disciplina correspondiente
Criterios de Valoración	Este método se considera complementario al SE1 en el sentido de que algunas de las actividades prácticas realizadas por los alumnos se evaluarán conjuntamente con los problemas. Los criterios de valoración son los mismos, por tanto, que en SE1.
Ponderación	0

Métodos / Instrumentos	SE7: Entrevista: Actividades individuales destinadas a comprobar la autoría de trabajos presentados, los conocimientos adquiridos, la destreza en procedimientos prácticos
Criterios de Valoración	El alumno deberá entregar un dossier con todo el trabajo realizado durante el curso (problemas, trabajos, etc) que será evaluado por el profesor y discutido con el alumno en una entrevista en la que éste deberá responder a las preguntas planteadas por el profesor. Para su valoración se tendrá en cuenta la corrección, rigor y claridad de las respuestas proporcionadas por el alumno a las preguntas planteadas por el profesor y la correcta utilización de los conceptos y herramientas matemáticos utilizados. La valoración de este instrumento de evaluación se hará de forma conjunta con SE1, pues la calificación del dossier de ejercicios presentado incluirá las conclusiones extraidas de la entrevista
Ponderación	10

Fechas de exámenes

https://www.um.es/web/estudios/masteres/matematica-avanzada/2023-24#examenes

9. Resultados del Aprendizaje

- Conocer las propiedades elementales del anillo de enteros Z, así como las principales aplicaciones de la factorización en producto de primos.

- Conocer las propiedades elementales del anillo de polinomios k[x], con k un cuerpo.

- Manejar la aritmética y las propiedades esenciales de las congruencias en Z.

- Conocer y manejar algunas de las funciones aritméticas más relevantes.

- Conocer los conceptos elementales de la criptografía tanto simétrica como asimétrica.

10. Bibliografía

Bibliografía Básica

Kenneth Ireland and Michael Rosen, A classical introduction to modern number theory. Graduate texts in Mathematics, Springer, 1990

David Burton, Elementary number theory (7th edition). Mc Graw Hill, 2011

Bibliografía Complementaria

Gareth A. Jones and J. Mary Jones, Elementary number theory, Springer Undergraduate Mathematics Series, 1998.

Michael Rosen, Elementary number theory and its applications. Pearson, 2023

Neal Koblitz, A course in number theory and criptography. Springer-Verlag, 1994

11. Observaciones y recomendaciones

Modalidad semipresencial. Los alumnos en modalidad semipresencial podrán asistir, previo acuerdo con el profesor, a todas las actividades por videoconferencia zoom. Además, se proporcionará el material necesario para poder preparar la asignatura de forma parcialmente autónoma, con asistencia del profesorado mediante tutorías presenciales o a distancia.

En esta modalidad y en las convocatroias extraordinarias el instrumento de evaluación SE5 no será evaluado y su porcentaje pasará a considarse dentro de SE1, el cual llegaría al 65 %.

Necesidades educativas especiales. Aquellos estudiantes con discapacidad o necesidades educativas especiales podrán dirigirse al Servicio de Atención a la Diversidad y Voluntariado (ADYV; http://www.um.es/adyv/) para recibir orientación sobre un mejor aprovechamiento de su proceso formativo y, en su caso, la adopción de medidas de equiparación y de mejora para la inclusión, en virtud de la Resolución Rectoral R-358/2016. El tratamiento de la información sobre este alumnado, en cumplimiento con la LOPD, es de estricta confidencialidad.”

Utilización de medios fraudulentos. Se aplicará el Artículo 23 (Utilización de medios fraudulentos) del Reglamento de convocatoria, evaluación y actas (Aprobado por el Consejo de Gobierno de la Universidad de

Murcia en sesión de 12 de abril de 2011), a pesar de su desafortunada redacción: "El estudiante que se valga o que realice conductas de las que pueda inferirse que pretende valerse de conductas, medios o instrumentos fraudulentos en la celebración de la prueba, incluida la indebida atribución de identidad o autoría, se le podrá suspender y, en su caso, podrá ser objeto de sanción previa apertura de expediente disciplinario."

Idioma. El inglés es el idioma de comunicación científica. Saber escribir, leer y hablar en inglés es esencial para comprender, aprender y comunicar la Ciencia, El material de referencia, tanto para la realización de los ejercicios como para la preparación de las exposiciones, estará escrito en inglés.