Proyecto/Guía docente de la asignatura Códigos Algebro-Geométricos

Asignatura	Códigos Algebro-Geométricos		
Materia	Matemáticas		
Módulo	Álgebra		
Titulación	Máster en Matemáticas		
Plan	645	**Código**	55023
Periodo de impartición	Primer cuatrimestre	**Tipo/Carácter**	Optativa
Nivel/Ciclo	Máster	**Curso**	Primero
Créditos ECTS	3		
Lengua en que se imparte	Castellano		
Profesor/es responsable/s	Diego Ruano Benito		
Datos de contacto (E-mail, teléfono…)	Email: diego.ruano@uva.es. Teléfono: 983185084. Despacho: A313 de la Facultad de Ciencias		
Departamento	Álgebra, Análisis Matemático, Geometría y Topología		

1. Situación / Sentido de la Asignatura

1.1 Contextualización

Los datos transmitidos a través de sistemas de comunicación digital pueden corromperse, lo que resulta en un desajuste entre los símbolos enviados y recibidos. Esto puede suceder en comunicaciones por satélite o teléfono móvil, en conexiones a través de internet y también cuando se almacenan datos en un ordenador o dvd.

Los códigos correctores de errores garantizan una transmisión fiable y rápida de información en dichos sistemas agregando símbolos adicionales a la información enviada. De esta forma, aunque algunos símbolos sean corrompidos, se puede recrear la información original gracias a la redundancia introducida. El desafío es construir códigos que, además de corregir muchos errores utilizando la menor cantidad de símbolos adicionales posible, también vengan acompañados de algoritmos rápidos de codificación y descodificación. Además, la teoría de códigos correctores tiene importantes aplicaciones en criptografía, entre ellas el criptosistema postcuántico de McEliece.

La geometría algebraica y los métodos combinatorios han demostrado ser herramientas fundamentales para tratar y describir los problemas que surgen en la construcción y uso de los códigos correctores de errores.

1.2 Relación con otras materias

Teoría de números, Álgebra conmutativa, Álgebra combinatoria, Seminario de álgebra, Geometría algebraica y Matemáticas de la Comunicación.

1.3 Prerrequisitos

Es recomendable, pero no imprescindible, tener conocimientos previos de teoría de códigos lineales y de las estructuras básicas del álgebra.

2. Competencias

2.1 Generales

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 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.
G1.- Conocimiento del método científico. Conocer el método científico, en particular en el ámbito de las Matemáticas, formulando modelos e hipótesis de trabajo relevantes y planificando el análisis en relación con dichas hipótesis y la discusión de las conclusiones, de modo que se pueda avanzar en el conocimiento de las Matemáticas.

G2.- Competencia para aplicar los conocimientos adquiridos. Aplicar los conocimientos técnicos adquiridos, de forma coherente y profesional, sobre todo en contextos novedosos o en constante renovación, que impliquen la realización de una actividad matemática.
G3.- Capacidad crítica, de análisis y síntesis, y capacidad de interpretación. Emitir juicios críticos sobre propuestas, hipótesis y validez científica de las conclusiones, así como sintetizar la presentación de propuestas y resultados, en el ámbito de las Matemáticas y de sus aplicaciones.
G4.- Competencias metodológicas. Elegir la metodología más adecuada para el desarrollo de la investigación de un problema, adaptándola al contexto en el que se origina el problema.
G5.- Capacidad para reconocer la originalidad y creatividad. Reconocer la originalidad en la concepción, formulación y resolución de problemas matemáticos.
G6.- Capacidades de comunicación. Presentar, de forma oral y escrita, y tanto ante públicos especializados como no especializados, resultados avanzados de investigación en Matemáticas, teniendo en cuenta los antecedentes en la investigación, las hipótesis de trabajo, los desarrollos y las conclusiones.
G7.- Capacidad de trabajo en equipo. Desarrollar una actividad matemática dentro de un equipo de investigación, bajo supervisión o de forma autónoma, pero al servicio de un proyecto investigador común.
G8.- Capacidad para el uso de las nuevas tecnologías. Adquirir destrezas generales en el uso de las nuevas tecnologías en el ámbito de la actividad matemática, facilitando su utilización en ámbitos diversos, así como el conocimiento de las herramientas informáticas disponibles más importantes.
G9.- Capacidad para poder mantener una formación permanente. Adquirir las destrezas necesarias para poder ampliar conocimientos y mantener una formación continua a lo largo de su vida profesional.
G10.- Capacidad de aprendizaje autónomo. Adquirir las destrezas necesarias para el aprendizaje autónomo en el ámbito de las Matemáticas, conociendo las fuentes de conocimiento para dicho aprendizaje y su utilización, y motivando el aprendizaje a lo largo de la vida en el ejercicio de la actividad matemática.
G11.- Competencias para la internacionalización de la actividad profesional en Matemáticas. Adquirir competencias que favorezcan el desarrollo de una actividad profesional en Matemáticas en contextos internacionales, especialmente mediante el uso de un idioma extranjero, usualmente el inglés, para la comunicación en el ámbito científico internacional de los resultados de la actividad investigadora.

2.2 Específicas

E1.- Adquisición de destrezas técnicas generales en el ámbito de una o varias áreas de las Matemáticas. Utilizar de forma profesional el lenguaje y las técnicas avanzadas propias de estas áreas, para favorecer la interpretación de las fuentes especializadas, así como la formulación adecuada de nuevos problemas.
E2.- Capacidad de comprensión de las bases teóricas y técnicas en las que se apoyan los conceptos y métodos de las materias propias de las Matemáticas. Adquirir el corpus teórico que sustenta los conceptos y métodos de las materias propias de alguna de las áreas de las Matemáticas, y la capacidad para un manejo experto y fluido de dichos conocimientos.
E3.- Capacidad para iniciarse en la investigación y/o aplicación de las Matemáticas. Adquirir competencias suficientes para iniciar un proyecto de investigación en alguna de las áreas de conocimiento de Matemáticas, de forma supervisada, y en particular, en relación con las líneas de investigación que se ofertan en el Programa de Doctorado en Matemáticas de la Universidad de Valladolid. Alternativamente conseguir competencias que le permitan la colaboración en proyectos interdisciplinares en los que el uso de las técnicas y el pensamiento matemáticos resultan fundamentales.
E4.- Capacidad y destrezas para la gestión de las fuentes bibliográficas de la investigación. Buscar y gestionar documentación y bibliografía especializada, en el ámbito específico de la especialización que le sea propia; usar ésta de modo racional y crítico para determinar el estado del arte en un determinado problema, y dominar los recursos bibliográficos pertinentes.
E5.- Capacidad de aplicar y adaptar los modelos teóricos y las técnicas específicas tanto a problemas abiertos en su línea de especialización, como a problemas provenientes de otros ámbitos ya sean científicos o técnicos. Adaptar los modelos teóricos propios de cada una de las disciplinas de las Matemáticas para el estudio de problemas abiertos relacionados o para el análisis de otros problemas provenientes de los ámbitos científicos, sociales o tecnológicos.
E6.- Capacidad de analizar problemas, detectando el posible uso de modelos matemáticos para contribuir a su comprensión y resolución. Analizar nuevas situaciones para identificar la aplicación de modelos matemáticos, existentes o de nuevo diseño, que contribuyan a la comprensión y solución de los problemas planteados.
E7.- Capacidad de exponer y defender proyectos y trabajos de investigación en el ámbito de sus líneas de especialización, así como de mantener debates científicos sobre los mismos, ya sean estos propios o adquiridos. Exponer y defender proyectos y trabajos de investigación en el ámbito propio de la especialización adquirida, tanto para defender las tesis propias como para debatir con juicio crítico con terceros.
E8.- Discernir entre las diferentes orientaciones de las técnicas específicas que concurren en la comprensión y resolución de un problema, comprendiendo la oportunidad y el uso de cada una de ellas individualmente, así como la cooperación entre ellas de cara a la resolución global del problema.
E9.- Capacidad de comprender nuevos avances y perspectivas científicas en el ámbito de la investigación en las líneas de su especialización. Comprender la formulación de nuevos avances y las perspectivas que éstos abren.

E10.- Capacidad de detectar líneas de trabajo emergentes en el ámbito de las Matemáticas o de sus aplicaciones, identificando la relación, origen e influencia con el estado de conocimiento propio de cada una de las especializaciones de las Matemáticas. Reconocer líneas de trabajo emergentes en el ámbito de las Matemáticas o de sus aplicaciones, identificando las interrelaciones existentes con cada una de las especialidades.
E11.- Capacidad para modelar matemáticamente fenómenos de la realidad y describir, en el ámbito de esos fenómenos, la relevancia de los resultados matemáticos. Proponer y ajustar modelos matemáticos en el estudio de problemas concretos, estudiando sus propiedades y la teoría matemática que sustenta su uso.
E12.- Capacidad para el ajuste de modelos matemáticos. Valorar la idoneidad de un modelo matemático en un problema concreto, estudiando sus propiedades y manejando las herramientas de ajuste y diagnóstico necesarias.
E13.- Capacidad para la utilización de las nuevas tecnologías en el ámbito de las Matemáticas y de sus aplicaciones. Utilizar métodos computacionales, según el ámbito de estudio de su especialidad, para explorar la frontera del conocimiento en las distintas disciplinas de las Matemáticas, así como en sus aplicaciones.
E14.- Conocimiento con carácter general del software matemático de carácter profesional en las distintas disciplinas de las Matemáticas, y capacidad para orientar su aplicación según las situaciones y comprender sus limitaciones. Conocer el software matemático profesional propio de cada especialidad para dirigir su aplicación en una variedad de situaciones, comprendiendo sus limitaciones, y adaptándolo cuando sea necesario.
E15.- Competencia para el diseño de técnicas computacionales y su análisis en los distintos ámbitos de las Matemáticas. Diseñar y analizar métodos computacionales en el ámbito de la Información y la Criptografía, y utilizarlos en las diversas aplicaciones en que son relevantes.
E16.- Adquirir recursos y destrezas para la comunicación de resultados en Matemáticas de forma clara, ante audiencias especializadas y no especializadas.

3. Objetivos

-Conocer y comprender la construcción y descodificación de códigos correctores de errores usando técnicas de geometría algebraica y álgebra computacional.

-Ser capaz de implementar la construcción y descodificación de códigos algebro-geométricos en sistemas de álgebra computacional.

-Conocer y comprender posibles aplicaciones de la teoría de códigos algebro-geométricos en criptografía.

4. Contenidos y/o bloques temáticos

Bloque 1: Códigos Algebro-Geométricos

Carga de trabajo en créditos ECTS: 3

a. Contextualización y justificación

Como se ha descrito en el apartado 1.1, los códigos correctores de errores son necesarios para la comunicación y almacenamiento de información digital.

Los códigos Reed-Solomon proporcionan códigos cuyos parámetros son excelentes, pero que se presentan la desventaja de necesitar un cuerpo finito grande para su implementación. Los códigos algebro-geométricos constituyen la principal alternativa para obtener códigos largos sobre un cuerpo finito. En particular, tomaron especial relevancia cuando fueron usados para proporcionar la primera sucesión infinita de códigos correctores con parámetros excelentes.

b. Objetivos de aprendizaje

Conocer y comprender la construcción y descodificación de códigos correctores de errores usando técnicas de geometría algebraica y álgebra computacional. Ser capaz de implementar su construcción y descodificación en sistemas de álgebra computacional. Conocer y comprender posibles aplicaciones de la teoría de códigos en criptografía.

c. Contenidos

Breve introducción a la teoría de códigos correctores. Breve introducción a curvas algebraicas. Construcción de códigos a partir de variedades algebraicas, especialmente curvas. Descodificación. Aplicaciones de códigos algebro-geométricos en criptografía.

d. Métodos docentes

Lecciones magistrales. Clases prácticas en el aula y con ordenador. Trabajos propuestos a los alumnos.

e. Plan de trabajo

Lecciones teóricas y prácticas que se complementaran con la realización de trabajos

f. Evaluación

Trabajos individuales y en grupo + exposición (80%) y examen final (20%)

g Material docente

g.1 Bibliografía básica

-A. Couvreur, H. Randriambololona. Algebraic Geometry codes and some applications. Chapter 15 in Concise Encyclopedia of Coding Theory. Ed. W.C. Huffman, J.L Kim, P. Solé. CRC Press (2021)

-T. Høholdt, J.H. van Lint, R. Pellikaan. Algebraic Geometry Codes. In the Handbook of Coding Theory, vol I, páginas 871-961 (Editores: V.S. Pless, W.C. Huffman and R.A. Brualdi). Elsevier (1998)

-C. Munuera, J. Tena. Codificación de la Información. Pub. Universidad de Valladolid (1997)

-M. Tsfasman, S. Vlăduţ, D. Nogin. Algebraic Geometry Codes: Basic Notions. Mathematical Surveys and Monographs. Volume 139. AMS (2007)

g.2 Bibliografía complementaria

-W.C. Huffman, V. Pless. Fundamentals of Error-Correcting Codes. Cambridge University Press (2003)

-E. Martínez-Moro, C. Munuera, D. Ruano. Advances in Algebraic Geometry Codes. Series on Coding Theory and Cryptology: Volume 5. World Scientific (2008)

-H. Niederreiter, C. Xing. Algebraic Geometry in Coding Theory and Cryptography. Princeton University Press (2009)

-H. Stichtenoth. Algebraic Function Fields and Codes. Graduate Texts in Mathematics 254. Second Edition. Springer Verlag (2009)

-M. Tsfasman, S. Vlăduţ, D. Nogin. Algebraic Geometry Codes: Advanced Chapters. Mathematical Surveys and Monographs. Volume 238. AMS (2019)

g.3 Otros recursos telemáticos (píldoras de conocimiento, blogs, videos, revistas digitales, cursos masivos (MOOC), …)

Páginas web de ayuda y foros de los sistemas de álgebra computacional Magma, Singular y Sage.

h. Recursos necesarios

Aula y ordenador con los sistemas de álgebra computacional Singular y Sage (libres y gratuitos).

i. Temporalización

CARGA ECTS	PERIODO PREVISTO DE DESARROLLO
3	Semanas 1-15

5. Métodos docentes y principios metodológicos

Se combinará la clase magistral junto con el aprendizaje basado en resolución de problemas.

6. Tabla de dedicación del estudiante a la asignatura

ACTIVIDADES PRESENCIALES o PRESENCIALES A DISTANCIA(1)	HORAS	ACTIVIDADES NO PRESENCIALES	HORAS
Clases teóricas	15	Estudio autónomo	25
Seminarios y clases con ordenador en el aula de informática, incluyendo presentación de trabajos y ejercicios propuestos	10	Preparación y redacción de ejercicios u otros trabajos	18
Sesiones de evaluación	2	Documentación: consultas bibliográficas, internet, …	5
Total presencial	**27**	Total no presencial	**48**
		TOTAL presencial + no presencial	**75**

(1) Actividad presencial a distancia es cuando un grupo sigue una videoconferencia de forma síncrona a la clase impartida por el profesor para otro grupo presente en el aula.

7. Sistema y características de la evaluación

Criterio: cuando al menos el 50% de los días lectivos del cuatrimestre transcurran en normalidad, se asumirán como criterios de evaluación los indicados en la guía docente. Se recomienda la evaluación continua ya que implica minimizar los cambios en la adenda.

INSTRUMENTO/PROCEDIMIENTO	PESO EN LA NOTA FINAL	OBSERVACIONES
Realización y exposición de trabajos	80%	
Examen final	20%	

CRITERIOS DE CALIFICACIÓN
• **Convocatoria ordinaria:** o Exactitud, claridad, precisión en la exposición de conceptos y cálculos. • **Convocatoria extraordinaria:** o Exactitud, claridad, precisión en la exposición de conceptos y cálculos.

8. Consideraciones finales