Datos identificativos							
Asignatura	Matemática Discreta Computacional					**Código**	0000
Enseñanza	Oficial					**Curso**	1
Descriptores	**Crd. total**	**Crd. T**	**Crd. P**	**Tipo**	**Periodo**	**Ciclo**	
	6	3	3	Mixto	Docencia	Master	
Idioma	Español						
Prerrequisitos	Conocimientos Álgebra Lineal y Álgebra Básica						
Departamento	Álgebra y Matemática Aplicada						
Coord./profesor	**J. C. Rosales González** P. A. García Sánchez A. Robles Juan Angel Aledo; José Carlos Valverde (UCLM)				**e-mail**	jrosales@ugr.es pedro@ugr.es arobles@ugr.es	
Web							
Descripción general	Curso dedicado a las aplicaciones de la Matemática Discreta y del Álgebra Computacional.						

Competencias	
Específicos (tipo A)	1. Aplicaciones de la aritmética modular tanto en matemáticas como en informática. Teorema chino del resto, y sus vertientes entera y polinomial 2. Descomposición de polinomios. Descomposición libre de cuadrados y algoritmo de Berlekamp 3. Aplicaciones de la aritmética modular en criptografía. RSA y Deffie-Hellman 4. Dualidad evaluación-interpolación de polinomios. Algoritmos de evaluación e interpolación rápida. La trasformada rápida de Fourier. Multiplicación rápida de enteros y polinomios 5. Sistemas de ecuaciones polinomiales. Fundamentos algebraicos: anillos de polinomios e ideales. Resolución de sistemas de ecuaciones y eliminación de variables 6. Aplicaciones geométricas y robóticas del algoritmo de Buchberger 7. Teoría de grafos y aplicaciones. Algoritmo de compresión de Huffman 8. Retículos y álgebras de Boole. Circuitos lógicos.
Transversales (Tipo B)	**Instrumentales** 1. Capacidad de análisis y síntesis 2. Capacidad de organización y planificación 3. Capacidad de comunicación oral y escrita 4. Conocimientos de informática relativos al ámbito de estudio 5. Capacidad de resolución de problemas **Personales** 6. Capacidad para trabajar en equipo y colaborar eficazmente con otras personas 7. Capacidad para trabajar en equipos de carácter interdisciplinar 8. Habilidades en las relaciones interpersonales 9. Razonamiento crítico **Sistémicas** 10. Capacidad para pensar de forma creativa y desarrollar nuevas ideas y conceptos 11. Iniciativa y espíritu emprendedor 12. Mostrar interés por la calidad de la propia actuación y saber desarrollar sistemas para garantizar la calidad de los propios servicios **Otras Competencias** 13. Capacidad para asumir responsabilidades 14. Capacidad de autocrítica: ser capaz de valorar la propia actuación de forma crítica 15. Saber valorar la actuación personal y conocer las propias competencias y limitaciones 16. Relaciones profesionales: ser capaz de establecer y mantener relaciones con otros profesionales e instituciones relevantes 17. Saber obtener información de forma efectiva a partir de libros y revistas especializadas, y de otra documentación
Nucleares (Tipo C)	Conocer los algoritmos básicos de la matemática discreta y del álgebra computacional Ser capaz de implementar dichos algoritmos en un lenguaje de programación funcional Conocer aplicaciones de dichos algoritmos en otras ramas de la ciencia

Objetivos de aprendizaje	Competencias relacionadas

Teorema chino del resto	Aplicaciones en representación modular de enteros. Interpolación de Newton.
Factorización de polinomios	Descomposición libre de cuadrados y algoritmo de Berlekamp. Interrelación del Teorema chino del resto con el Álgebra Lineal.
Aplicaciones a la Criptografía	Teorema pequeño de Fermat. Teorema de Lagrange. Teorema de Euler. RSA y Deffie-Hellman.
Evaluación e interpolación de polinomios	Dualidad evaluación e interpolación. Raices n-ésimas de la unidad complejas y en cuerpos finitos. Transformada rápida de Fourier. Multiplicación rápida de enteros y polinomios.
Algoritmo de Buchberger para el cálculo de Bases de Gröbner	Eliminación de variables en sistemas de ecuaciones polonomiales. Resolución de sistemas de ecuaciones.
Implicitación y parametrización	Aplicaciones geométricas. Brazos de robot.
Teoría de grafos	Problemas de planificación. Algoritmos de compresión y búsqueda.
Retículos y álgebras de Boole	Circuitos lógicos y de conmutación.

CONTENIDOS	
Bloque/tema/módulo	**Descripción**
1	Ecuaciones diofánticas. Soluciones naturales. Teorema chino del resto, y sus vertientes entera y polinomial. Algoritmo de Garner y de Newton.
2	Descomposición de polinomios. Descomposición libre de cuadrados y algoritmo de Berlekamp. Levantamiento de Hensel.
3	Aplicaciones de la aritmética modular en criptografía. Teorema de Fermat. Teorema de Euler. RSA. Cálculo de elementos primitivos. Deffie-Hellman.
4	Evaluación-interpolación de polinomios. Algoritmos de evaluación e interpolación rápida. Raices de la unidad. La trasformada rápida de Fourier. Multiplicación rápida de enteros y polinomios.
5	Sistemas de ecuaciones polinomiales. Fundamentos algebraicos: anillos de polinomios e ideales. Órdenes monomiales. Algoritmo de Buchberger. El problema de palabras. Eliminación de variables. Modelización y programación de brazos de robot. El problema de la cinemática directa e inversa.
6	Teoría de grafos y aplicaciones. Algoritmos de compresión y búsqueda. Compresión de Huffman.
7	Retículos y Álgebras de Boole. Aplicaciones al diseño de circuitos conmutadores y lógicos.

METODOLOGÍA

Tipología	Descripción
Presentación	Entrevista personal a cada alumno matriculado por el Profesorado del curso acerca de sus intereses y expectativas en el campo de estudio del curso
Lecciones magistrales	30 horas sobre los contenidos del curso.
Acontecimientos científicos o divulgativos	Asistencia a posibles conferencias sobre temas relacionados con el curso Contacto con otros grupos de investigación que utilicen técnicas semejantes o desarrollen investigaciones relacionadas
Prácticas de laboratorio	Implementación de los algoritmos estudiados en Mathematica
Prácticas autónomas	Realización de un trabajo personal sobre un tema elegido por el alumno sobre los tópicos del curso. Revisión bibliográfica de antecedentes, metodología y recursos y elaboración de un posible trabajo de investigación (hipótesis, antecedentes, objetivos, diseño experimental, metodología, etc.)
Prácticas a través de TIC	Visita, crítica e informe acerca de los contenidos de distintos portales Web de grupos de investigación que trabajen en los diferentes temas del curso.
Prácticas externas (de campo/salidas)	

			A	B	C	D	E
Tipología de la actividad *Que se hace en la asignatura?*	**Atención personalizada** *La actividad implica atención personalizada*	**Evaluación** *Tiene implicación en la cualificación?*	**Horas de clase** *Aula ordinaria*	**Horas presenciales fuera del aula** *Entorno académico guiado*	**Factor de Trabajo del alumno**	**Horas de trabajo personal del alumno** *(A o B xC)*	**Horas totales** *(A+B+D)*
Actividades introductorias	Entrevista	Encuesta final al alumno	0	1	0	1	1
Lección magistral	Tutorías	Cuestionario	30	0	1'25	37'5	67'5
Acontecimientos científicos o divulgativos	Comunicación, puesta en contacto con otros grupos	Resumen de la conferencia o informe del responsable del grupo de investigación visitado	0	5	1	5	10
Prácticas de laboratorio y autónomas	Seguimiento en el laboratorio	Desarrollo de un experimento Realización de un trabajo y proyecto tutorizado	30	0	1.5	45	75
Prácticas externas (de campo/salidas)							
Atención personalizada	Tutorías de teoría y prácticas autónomas		0	4	0	4	4
							157'5

ATENCIÓN PERSONALIZADA	
Tipología	**Descripción**
Tutoría	Las tutorías se realizarán durante el periodo comprendido entre el inicio de curso y el final del Master. Las vías de comunicación serán tanto presenciales como a través de TIC (correo electrónico, foros, etc.)

EVALUACIÓN		
Tipología	**Descripción**	**%**

Evaluación continua	Evaluación teórica Prácticas de laboratorio (aprovechamiento, iniciativa, habilidades) Prácticas Autónomas: Trabajo tutelado y Proyecto de investigación	20 30 50

Fuentes de información	
Básica	- W. W. Adams y P. Loustaunau, An introduction to Gröbner bases, A.M.S. G. S. in M., volumen 4. - A. G. Akritas, Elements of computer algebra with applications, John Wiley & Sons, 1989. - R. J. Gaylord, S. N. Kamin y P. R. Wellin, An introduction to programming with Mathematica. Springer-Verlag/Telos, 1996. - K. O. Geddes, S. R. Czapor, G. Labahn, Algorithms for computer algebra, Kluwer Academic Publishers, 1992. - J. Grabmeier, E. Kaltofen, V. Weispfenning, Computer Algebra Handbook, Springer. - S. Wolfram, The Mathematica book, 3ª edición, Cambridge Univeristy Press, 1998. - C. K. Yap, Fundamental problems of algorithmic algebra, Oxford University Press - Joachim von zur Gathen y Jürgen Gerhard, Modern Computer Algebra, Springer **http://www-math.uni-paderborn.de/mca/**
Complementaria	Red EACA **http://www.unirioja.es/dptos/dmc/RedEACA/presentacionEACA.html** Symbolic mathematical computation information center **http://www.symbolicnet.org/** Research institute for symbolic computation **http://www.risc.uni-linz.ac.at/** Handbook of applied cryptography **http://www.cacr.math.uwaterloo.ca/hac/**
Otros recursos	Journal of symbolic computation http://www.elsevier.com/wps/find/journaldescription.cws_home/622902/description#description Ontario Research Centre for Computer Algebra http://www.orcca.on.ca/ Mathematics of Computation http://www.ams.org/journals/mcom/

Recomendaciones