ANX-PR/CL/001-01

GUÍA DE APRENDIZAJE

ASIGNATURA

105000451 - álgebra Aplicada Y Computacional

PLAN DE ESTUDIOS

10ML - Grado En Matematicas E Informática

CURSO ACADÉMICO Y SEMESTRE

2022/23 - Segundo semestre

Índice

Guía de Aprendizaje

1. Datos descriptivos

1.1. Datos de la asignatura

Nombre de la asignatura	105000451 - álgebra Aplicada y Computacional
No de créditos	6 ECTS
Carácter	Optativa
Curso	Cuarto curso
Semestre	Octavo semestre
Período de impartición	Febrero-Junio
Idioma de impartición	Castellano
Titulación	10ML - Grado en Matematicas e Informática
Centro responsable de la titulación	10 - Escuela Tecnica Superior De Ingenieros Informaticos
Curso académico	2022-23

2. Profesorado

2.1. Profesorado implicado en la docencia

Nombre	Despacho	Correo electrónico	Horario de tutorías *
Juan Angel Rojo Carulli (Coordinador/a)	1302	juan.rojo.carulli@upm.es	Sin horario. Cita previa.
Alfonso Zamora Saiz	1312	alfonso.zamora@upm.es	Sin horario. Cita previa.

* Las horas de tutoría son orientativas y pueden sufrir modificaciones. Se deberá confirmar los horarios de tutorías con el profesorado.

3. Conocimientos previos recomendados

3.1. Asignaturas previas que se recomienda haber cursado

- Geometria Afin Y Proyectiva

- Estructuras Algebraicas

3.2. Otros conocimientos previos recomendados para cursar la asignatura

El plan de estudios Grado en Matematicas e Informática no tiene definidos otros conocimientos previos para esta asignatura.

4. Competencias y resultados de aprendizaje

4.1. Competencias

CE26 - Conocimiento de los tipos apropiados de soluciones, y comprensión de la complejidad de los problemas informáticos y la viabilidad de su solución.

CE43 - Capacidad para trabajar de forma efectiva como individuo, organizando y planificando su propio trabajo, de forma independiente o como miembro de un equipo.

CG01 - Capacidad de resolución de problemas aplicando conocimientos de matemáticas, ciencias e ingeniería.

CG02 - Capacidad para el aprendizaje autónomo y la actualización de conocimientos, y reconocimiento de su necesidad en las áreas de la matemática y la informática.

CG05 - Capacidad de abstracción, análisis y síntesis.

CG08 - Capacidad de comunicarse de forma efectiva con los compañeros, usuarios (potenciales) y el público en general acerca de cuestiones reales y problemas relacionados con la especialización elegida.

CG10 - Capacidad para usar las tecnologías de la información y la comunicación.

4.2. Resultados del aprendizaje

RA189 - Estudio de las bases de Gröbner y de sus aplicaciones en el diseño de algoritmos.

RA191 - Comprensión de las relaciones entre el álgebra abstracta y la computación, y de sus aplicaciones.

RA190 - Estudio de las curvas elípticas y de sus aplicaciones en computación y criptografía.

RA102 - Desarrollar la solución matemática y algorítmica mas apropiada a un problema matemático o informático que requiera un tratamiento especialmente complejo, analizando y exponiendo su viabilidad.

RA111 - Dado un campo de aplicación de las matemáticas o de la informática, evaluar y diseñar la solución más apropiada para resolver alguno de sus problemas, exponiendo las dificultades técnicas y los limites de la aplicación

RA103 - Conocer alguno de los campos situados en la frontera entre las matemáticas y la informática, que están en la base de nuevas tendencias y desarrollos.

RA104 - Dado un campo de aplicación de las matemáticas o de la informática, evaluar y diseñar la solución más apropiada para resolver alguno de sus problemas, exponiendo las dificultades técnicas y los limites de la aplicación.

RA105 - Dado un problema real elegir las herramientas matemáticas o la tecnología informática más apropiada para su solución y diseñar su desarrollo e integración, analizando la viabilidad de su solución.

5. Descripción de la asignatura y temario

5.1. Descripción de la asignatura

En esta asignatura se introducen algunas nociones avanzadas de álgebra y geometría que tienen importantes aplicaciones en el área de la computación. Una de ellas son las **bases de Gröbner**, imprescindibles para calcular y trabajar con ideales en anillos de polinomios, así como para resolver sistemas de ecuaciones polinomiales no lineales. Las bases de Gröbner tienen numerosas aplicaciones en la resolución de problemas modelados con este tipo de ecuaciones, como pueden ser la búsqueda de soluciones de un juego (tipo Sudoku), coloraciones de grafos, y en general todo problema con restricciones que sea traducible a un sistema de ecuaciones polinómicas.

Otra interracción importante entre la geometría algebraica y la computación se da en las llamadas **curvas elípticas**. Este tipo de curvas algebraicas poseen una estructura no trivial de grupo conmutativo relacionada con sus propiedades álgebro-geométricas. Esta estructura es muy interesante, y posibilita que estas curvas sean utilizadas para resolver problemas computacionales relacionados con la factorización de números enteros, factorización que tiene especial interés debido a sus aplicaciones para la codificación y la transmisión de información. Adicionalmente, juegan un papel relevante en la fundamentación teórica de importantes sistemas de encriptación de mensajes, dando lugar a una rama que en inglés se conoce como Elliptic-curve cryptography.

Se espera que los alumnos se familiaricen con la teoría matemática básica para entender los conceptos fundamentales de la geometría algebraica, y que puedan realizar cálculos efectivos en sus diversas aplicaciones a problemas concretos, por medio de la programación de los algoritmos más relevantes relacionados con las bases de Grobner y las curvas elípticas.

5.2. Temario de la asignatura

1. Variedades afines y proyectivas.
   1.1. Anillos de polinomios e ideales. Homogeneización de polinomios.
   1.2. Variedades. Completada proyectiva de una variedad afín.
   1.3. Correspondencia entre variedades e ideales.
   1.4. Bases de Gröbner y teorema de la base de Hilbert.
2. Propiedades y aplicaciones de las bases de Gröbner.
   2.1. Algoritmo de Buchberger para la construcción de bases de Gröbner.
   2.2. Algoritmo de división asociado a una base de Gröbner.
   2.3. El problema de pertenencia a un ideal. Eliminación de variables.
   2.4. Eliminación de variables y resolución de sistemas de ecuaciones polinomiales.
3. Curvas algebraicas afines y proyectivas.
   3.1. Parametrizaciones de curvas.
   3.2. Puntos singulares y regulares.
   3.3. Intersección de curvas y Teorema de Bézout.
   3.4. El género de una curva.
4. Curvas elípticas.
   4.1. Ecuación de Weirstrass de una curva elíptica.
   4.2. Estructura de grupo conmutativo.
   4.3. Algoritmos para la suma de puntos.
5. Curvas elípticas sobre cuerpos finitos.
   5.1. Acotación y cálculo del número de puntos.
   5.2. Algoritmo de Lenstra para la factorización de números enteros.
   5.3. Tests de primalidad basados en curvas elípticas. Algoritmo de Atkin-Morain.
   5.4. El problema del logaritmo discreto.

6. Cronograma

6.1. Cronograma de la asignatura *

Sem	Actividad en aula	Actividad en laboratorio	Tele-enseñanza	Actividades de evaluación
1	**Explicación de contenidos teóricos del Tema 1.** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Práctica 1.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio			
2	**Explicación de contenidos teóricos del Tema 1.** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Práctica 1.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio			
3	**Explicación de contenidos teóricos del Tema 1.** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Práctica 1.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio			
4	**Explicación de contenidos teóricos del Tema 2.** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Práctica 1.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio			**Entrega Práctica 1.** TI: Técnica del tipo Trabajo Individual Evaluación continua No presencial Duración: 00:00
5	**Explicación de contenidos teóricos del Tema 2.** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Práctica 2.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio			

6	**Explicación de contenidos teóricos del Tema 2.** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Práctica 2.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio			
7	**Explicación de contenidos teóricos del Tema 3.** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Práctica 2.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio			
8	**Explicación de contenidos teóricos del Tema 3.** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Práctica 2.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio			**Entrega Práctica 2.** TI: Técnica del tipo Trabajo Individual Evaluación continua No presencial Duración: 00:00
9	**Explicación de contenidos teóricos del Tema 3.** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Práctica 3.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio			
10	**Explicación de contenidos teóricos del Tema 4.** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Práctica 3.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio			
11	**Explicación de contenidos teóricos del Tema 4.** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Práctica 3.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio			

12	**Explicación de contenidos teóricos del Tema 4.** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Práctica 4.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio			**Entrega Práctica 3.** TI: Técnica del tipo Trabajo Individual Evaluación continua No presencial Duración: 00:00
13	**Explicación de contenidos teóricos del Tema 5.** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Práctica 4.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio			
14	**Explicación de contenidos teóricos del Tema 5.** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Práctica 4.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio			
15	**Explicación de contenidos teóricos del Tema 5.** Duración: 02:00 LM: Actividad del tipo Lección Magistral **Práctica 4.** Duración: 02:00 PL: Actividad del tipo Prácticas de Laboratorio			**Entrega Práctica 4.** TI: Técnica del tipo Trabajo Individual Evaluación continua No presencial Duración: 00:00
16				
17				**Prueba de Evaluación Final.** EX: Técnica del tipo Examen Escrito Evaluación sólo prueba final Presencial Duración: 03:00 **Presentación Final de las Prácticas.** PI: Técnica del tipo Presentación Individual Evaluación continua Presencial Duración: 03:00

Para el cálculo de los valores totales, se estima que por cada crédito ECTS el alumno dedicará dependiendo del plan de estudios, entre 26 y 27 horas de trabajo presencial y no presencial.

* El cronograma sigue una planificación teórica de la asignatura y puede sufrir modificaciones durante el curso derivadas de la situación creada por la COVID-19.

7. Actividades y criterios de evaluación

7.1. Actividades de evaluación de la asignatura

7.1.1. Evaluación (progresiva)

Sem.	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
4	Entrega Práctica 1.	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	20%	5 / 10	CG01 CG02 CG05 CE26 CE43 CG10 CG08
8	Entrega Práctica 2.	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	20%	5 / 10	CG01 CG02 CG05 CE26 CG08 CG10 CE43
12	Entrega Práctica 3.	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	20%	5 / 10	CG01 CG02 CG05 CE26 CG08 CG10 CE43
15	Entrega Práctica 4.	TI: Técnica del tipo Trabajo Individual	No Presencial	00:00	20%	5 / 10	CG01 CG02 CG05 CE26 CG08 CG10 CE43
17	Presentación Final de las Prácticas.	PI: Técnica del tipo Presentación Individual	Presencial	03:00	20%	5 / 10	CG01 CG02 CG05 CE26 CE43 CG10 CG08

7.1.2. Prueba evaluación global

Sem	Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
17	Prueba de Evaluación Final.	EX: Técnica del tipo Examen Escrito	Presencial	03:00	100%	5 / 10	CG01 CG02 CG05 CE26 CG08 CG10 CE43

7.1.3. Evaluación convocatoria extraordinaria

Descripción	Modalidad	Tipo	Duración	Peso en la nota	Nota mínima	Competencias evaluadas
Examen convocatoria extraordinaria.	EX: Técnica del tipo Examen Escrito	Presencial	03:00	100%	5 / 10	CG01 CG02 CG05 CE26 CG08 CG10 CE43

7.2. Criterios de evaluación

Convocatoria ordinaria: Sistema general de evaluación continua: Las actividades evaluables son las especificadas en la tabla del apartado anterior, cada una de ellas puntuable de 0 a 10. Consistirán en las entregas parciales y secuenciadas de las prácticas del curso y de su presentación oral en la fecha del examen marcada por el centro. La nota de la asignatura se calcula según los pesos fijados en dicha tabla, y se considera aprobada la asignatura cuando se obtiene una nota mayor o igual que 5 sobre 10.

Los alumnos que no entreguen las prácticas en las fechas indicadas, tendrán la opción de entregarlas y presentarlas en la Prueba de Evaluación Final, en la fecha marcada por el centro. La calificación de esta prueba global será la de la asignatura.

Convocatoria extraordinaria de julio: El alumnado deberá entregar las prácticas del curso y presentarlas oralmente. La calificación de esta prueba global será la de la asignatura. Se considera aprobada la asignatura cuando se obtiene una nota mayor o igual que 5 sobre 10.

8. Recursos didácticos

8.1. Recursos didácticos de la asignatura

Nombre	Tipo	Observaciones
Ideals, Varieties and Algorithms, David A. Cox, John Little, Donal O'Shea. Springer, 2015.	Bibliografía	
The Arithmetic of Elliptic Curves, Joseph H. Silverman. Springer, 2nd edition 2008.	Bibliografía	
An introduction to Mathematical Cryptography, Jeffrey Hoffstein, Jill Pipher, Joseph H. Silverman. Springer, 2010.	Bibliografía	

An Introduction to Gröbner Bases, William W. Adams, Philippe Loustaunau. AMS, 1994.	Bibliografía	
Algebraic Curves, William Fulton, W.A. Benjamin, Inc, 1969.	Bibliografía	
Rational Points on Elliptic Curves, Joseph H. Silverman, John T. Tate. Springer, 2nd Edition 2015.	Bibliografía	
Material accesible en Moodle.	Recursos web	