GUÍA DOCENTE

HERRAMIIENTAS COMPUTACIONALES PARA LA RESOLUCIÓN DE PROBLEMAS

Coordinación: MIRET BIOSCA, JOSE MARIA

Año académico 2017-18

HERRAMIIENTAS COMPUTACIONALES PARA LA RESO... 2017-18

Información general de la asignatura

<table>
<tr><td>Denominación</td><td>HERRAMIIENTAS COMPUTACIONALES PARA LA RESOLUCIÓN DE PROBLEMAS</td></tr>
<tr><td>Código</td><td>102042</td></tr>
<tr><td>Semestre de impartición</td><td>1R Q(SEMESTRE) EVALUACIÓN CONTINUADA</td></tr>
<tr><td>Carácter</td><td>
<table>
<tr><th>Grado/Máster</th><th>Curso</th><th>Carácter</th><th>Modalidad</th></tr>
<tr><td>Grado en Ingeniería Informática</td><td>4</td><td>OBLIGATORIA</td><td>Presencial</td></tr>
</table>
</td></tr>
<tr><td>Número de créditos ECTS</td><td>6</td></tr>
<tr><td>Grupos</td><td>1GG</td></tr>
<tr><td>Créditos teóricos</td><td>3</td></tr>
<tr><td>Créditos prácticos</td><td>3</td></tr>
<tr><td>Coordinación</td><td>MIRET BIOSCA, JOSE MARIA</td></tr>
<tr><td>Departamento/s</td><td>MATEMATICA</td></tr>
<tr><td>Distribución carga docente entre la clase presencial y el trabajo autónomo del estudiante</td><td>150 horas de trabajo
60 horas declase presencial
90 horas de trabajo autónomo</td></tr>
<tr><td>Información importante sobre tratamiento de datos</td><td>Consulte este enlace para obtener más información.</td></tr>
<tr><td>Idioma/es de impartición</td><td>Inglés</td></tr>
<tr><td>Horario de tutoría/lugar</td><td>Concertar cita por correo electrónico.</td></tr>
</table>

HERRAMIIENTAS COMPUTACIONALES PARA LA RESO... 2017-18

Profesor/a (es/as)	Dirección electrónica profesor/a (es/as)	Créditos impartidos por el profesorado	Horario de tutoría/lugar
MIRET BIOSCA, JOSE MARIA	miret@matematica.udl.cat	2,5	
PUJOLAS BOIX, JORDI	jpujolas@matematica.udl.cat	3,5	Miércoles 19:00 - 20:00 Despacho 1.20 EPS A concertar por correo electrónico.
GARRA ORONICH, RICARD JOSEP	garra@matematica.udl.cat	1,2	

Información complementaria de la asignatura

Requisitos previos: Álgebra, Estadística y Optimización, Programación 1.

Objetivos académicos de la asignatura

Los resultados de aprendizaje que el estudiante tiene que alcanzar en esta asignatura son:

- Solucionar sistemas de ecuaciones lineales por diferentes métodos directos: Gauss, LU y QR.
- Determinar los valores y vectores propios de una matriz cuadrada.
- Solucionar sistemas de ecuaciones lineales por métodos iterativos y conocer sus condiciones de convergencia.
- Conocer y utilizar las transformaciones geométricas del plano más habituales para desplazar objetos.
- Determinar el polinomio de interpolación de un conjunto de puntos del plano.
- Distribuir fragmentos de una clave mediante el esquema para compartir secretos de Shamir.
- Conocer y usar adecuadamente algoritmos de factorización y tests de primalidad.
- Cifrar, descifrar y firmar digitalmente con el criptosistema RSA y el criptosistema ElGamal.
- Adquirir habilidades para resolver problemas computacionales mediante el software matemático SAGE.

Competencias

Competencias específicas de la titulación.

- GII-C1. Capacidad para tener un conocimiento profundo de los principios fundamentales y modelos de la computación y saberlos aplicar para interpretar, seleccionar, valorar, modelar, y crear nuevos conceptos, teorías, usos y desarrollos tecnológicos relacionados con la informática.
- GII-C3. Capacidad para evaluar la complejidad computacional de un problema, conocer estrategias algorítmicas que puedan conducir a su resolución y recomendar, desarrollar e implementar aquella que garantice el mejor rendimiento de acuerdo con los requisitos establecidos.

Competencias transversales de la titulación.

- EPS6. Capacidad de análisis y síntesis.

Competencias estratégicas de la UdL.

- CT2. Adquirir un dominio significativo de una lengua extranjera, especialmente del inglés.

- CT3. Adquirir capacitación en el uso de las nuevas tecnologías y de las tecnologías de la información y la comunicación.

Contenidos fundamentales de la asignatura

1. Sistemas de ecuaciones lineales.
    1. Formulación matricial.
    2. Método de Gauss.
    3. Factorización LU.
    4. Factorización QR.
    5. Norma de una matriz.
    6. Valores y vectores propios de matrices cuadradas.
    7. Métodos iterativos.
    8. El algoritmo PageRank.
2. Transformaciones geométricas en el plano.
    1. Transformaciones básicas.
    2. Representación matricial y coordenadas homogéneas.
    3. Transformaciones inversas.
3. Interpolación polinómica.
    1. El anillo de polinomios.
    2. El algoritmo de Euclides para polinomios.
    3. Interpolación polinómica: el método de Lagrange.
    4. Esquemas para compartir secretos: el esquema de Shamir.
4. Aritmética modular.
    1. Anillos de clases de residuos
    2. Cuerpos finitos.
    3. Tests de primalidad.
    4. Algoritmos de factorización.
5. Introducción a la Criptografía.
    1. Criptosistemas simétricos.
    2. Criptosistemas de clave pública.
    3. El problema de la factorización de enteros.
    4. El criptosistema RSA.
    5. El problema del logaritmo discreto.
    6. El criptosistema ElGamal.
    7. Firmas digitales.
    8. Criptografía con curvas elípticas.

Ejes metodológicos de la asignatura

Se combinan clases de teoría, clases de problemas y clases con el software de cálculo simbólico SAGE. Las clases de teoría aportan los conceptos básicos de la asignatura, incorporando ejemplos ilustrativos que facilitan la comprensión. En las clases de problemas se combinan la resolución conjunta en la pizarra con la resolución individual y en grupo de los estudiantes en el aula.

Plan de desarrollo de la asignatura

Semana	Descripción	Actividad presencial	Trabajo autónomo
1	Introducción. Sistemas de ecuaciones lineales.	Presentación de la asignatura. 1.1, 1.2: Método de Gauss.	Estudiar la bibliografia i el plan de la asignatura.

2	Sistemas de ecuaciones lineales.	1.3, 1.4: Descomposiciones QR y LU.	Ejercicios y problemas en SAGE.
3	Sistemas de ecuaciones lineales.	1.5,1.6, 1.7: Métodos iterativos.	El algoritmo Page Rank.
4	Transformaciones geométricas en el plano.	2.1: Transformaciones básicas en el plano.	Ejercicios y problemas en SAGE.
5	Transformaciones geométricas en el plano.	2.2, 2.3: Formulación matricial y transformaciones inversas.	Transformaciones en el plano en SAGE.
6	Interpolación polinómica.	3.1, 3.2: Anillos de polinomios. El algoritmo de Euclides en anillos de polinomios.	Ejercicios y problemas en SAGE.
7	Interpolación polinómica.	3.3, 3.4: Interpolación. Interpolación de Lagrange. El esquema de Shamir de compartición de secretos.	Ejercicios y problemas en SAGE. El esquema de Shamir en SAGE.
8	Aritmética modular.	4.1, 4.2: Anillos de clases de residuos. Cuerpos finitos.	Ejercicios y problemas en SAGE.
9		**1er Examen Parcial**	Preparación de examen.
10	Aritmética modular.	4.3, 4.4: Primalidad y factorización.	Ejercicios y problemas en SAGE.
11	Introducción a la criptografía.	5.1,5.2: Nociones básicas de criptografía.	Ejercicios y problemas en SAGE.
12	Introducción a la criptografía.	5.3, 5.4: Factorización y RSA.	El criptosistema RSA en SAGE.
13	Introducción a la criptografía.	5.5, 5.6: Logaritmos discretos y cifrado de El Gamal.	El cifrado de El Gamal en SAGE.
14	Introducción a la criptografía.	5.7: Firma digital.	Ejercicios y problemas en SAGE.
15	Introducción a la criptografía.	5.8: Criptografía con curvas elípticas.	Ejercicios y problemas en SAGE.
16		**2o Examen Parcial**	Preparación de examen.
17		**2o Examen Parcial**	Preparación de examen.
18		Exposiciones orales.	Preparación de presentaciones orales.
19		**Recuperación**	Preparación examen.

Sistema de evaluación

Abr.	Actividad de evaluación	Ponderación	Nota mínima	En grupo	Obligatoria	Recuperable
C1	Práctica de SAGE	10%	NO	NO	SI	NO
P1	1r Examen Parcial	40%	1.5	NO	SI	SI
C2	Presentación oral	10%	NO	SI (<=2)	SI	NO

P2	2o Examen Parcial	40%	1.5	NO	SI	SI
PCL	Participación en classe	0,5 puntos	NO	NO	NO	NO
Los exámenes parciales, la práctica de SAGE y la presentación oral son obligatorios.						
Nota Final = 0,1*C1 + 0,4*P1 + 0,1*C2 + 0,4*P2 + 0,05*PCL						

La asignatura se supera si la nota final es igual a 5 o superior. La nota final es la suma ponderada de los exámenes parciales, la práctica de SAGE, de la presentación oral y adicionalmente de un máximo de 0,5 puntos de participación en classe y avaluación contínua. Los exámenes parciales son por escrito, tienen un peso del 40% sobre la nota final cada uno de ellos y tienen una nota mínima de 1,5 puntos para a ser evaluables. Los exámenes parciales, la práctica de SAGE y la presentación oral son obligatorios. Se pueden obtener hasta 0,5 puntos extras por una participación activa en clase y por otras actividades de evaluación contínua que serán debidamente anunciadas. El examen de recuperación consta del 1er o del 2o parcial o de ambos, a criterio del estudiante.

Bibliografía y recursos de información

H. Anton, Elementary Linear Algebra. Ed. John Wiley & Sons, 1994.

A. Aubanell, A. Benseny, A. Delshams, Eines bàsiques de Càlcul Numèric, Ed. Manuals UAB, 1991.

D.M. Bressoud, Factorization and Primality Testing. Ed. Springer, 1989.

L. Childs, A Concrete Introduction to Higher Algebra. Ed. Springer, 1988.

S. Lang, Algebra. Ed. Addison-Wesley, 1999.

R. Lidl, H. Niederreiter, Finite Fields, Ed. Cambridge University Press, 2003.

W. Stein, Elementary Number Theory: Primes, Congruences and Secrets. Ed. springer, 2009.

J. Stoer, R. Bulirsch, Introduction to Numerical Analysis, Springer, 1993.