



Universitat de Lleida

GUIA DOCENT  
**EINES COMPUTACIONALS PER  
A LA RESOLUCIÓ DE  
PROBLEMES**

Coordinació: MIRET BIOSCA, JOSE MARIA

Any acadèmic 2017-18

## Informació general de l'assignatura

<b>Denominació</b>	EINES COMPUTACIONALS PER A LA RESOLUCIÓ DE PROBLEMES			
<b>Codi</b>	102042			
<b>Semestre d'impartició</b>	1R Q(SEMESTRE) AVALUACIÓ CONTINUADA			
<b>Caràcter</b>	Grau/Màster	Curs	Caràcter	Modalitat
	Grau en Enginyeria Informàtica	4	OBLIGATÒRIA	Presencial
<b>Nombre de crèdits ECTS</b>	6			
<b>Grups</b>	1GG			
<b>Crèdits teòrics</b>	3			
<b>Crèdits pràctics</b>	3			
<b>Coordinació</b>	MIRET BIOSCA, JOSE MARIA			
<b>Departament/s</b>	MATEMATICA			
<b>Distribució càrrega docent entre la classe presencial i el treball autònom de l'estudiant</b>	150 hores de treball 60 hores de classe presencial 90 hores de treball autònom			
<b>Informació important sobre tractament de dades</b>	Consulteu <a href="#">aquest enllaç</a> per a més informació.			
<b>Idioma/es d'impartició</b>	Inglés			
<b>Horari de tutoria/lloc</b>	Concertar cita por correo electrónico.			

Professor/a (s/es)	Adreça electrònica professor/a (s/es)	Crèdits impartits pel professorat	Horari de tutoria/lloc
MIRET BIOSCA, JOSE MARIA	miret@matematica.udl.cat	2,5	
PUJOLAS BOIX, JORDI	jpujolas@matematica.udl.cat	3,5	Dimecres 19:00 - 20:00 Despatx 1.20 EPS A concertar per correu electrònic.
GARRA ORONICH, RICARD JOSEP	garra@matematica.udl.cat	1,2	

## Informació complementària de l'assignatura

Requisits previs: Àlgebra, Estadística i Optimizació, Programació 1.

## Objectius acadèmics de l'assignatura

Els resultats d'aprenentatge que l'estudiant ha d'assolir en esta assignatura són:

- Solucionar sistemes d'equacions lineals amb diferents mètodes directes: Gauss, LU i QR.
- Determinar els valors i vectors propis d'una matriu quadrada.
- Solucionar sistemes d'equacions lineals amb mètodes iteratius i conèixer les seves condicions de convergència.
- Conèixer i utilitzar les transformacions geomètriques del pla més habituals per a desplaçar objectes.
- Determinar el polinomi interpolador d'un conjunt de punts del pla.
- Distribuir fragments d'una clau mitjançant l'esquema de compartició de secrets de Shamir.
- Conèixer i emprar adequadament algorismes de factorització i tests de primalitat.
- Xifrar, desxifrar i signar digitalment amb el criptosistema RSA i el criptosistema d'ElGamal.
- Adquirir habilitats per a resoldre problemes computacionals amb el software matemàtic SAGE.

## Competències

Competències específiques de la titulació.

- GII-C1. Capacitat per tenir un coneixement profund dels models de la computació i dels seus principis fonamentals, i saber-los aplicar per a interpretar, seleccionar, valorar, modelar, i crear nous conceptes, teories, usos i desenvolupaments tecnològics relacionats amb la informàtica.
- GII-C3. Capacitat per a avaluar la complexitat computacional d'un problema, conèixer estratègies algorítmiques que puguin portar a la seva resolució i recomenar, desenvolupar i implementar aquella que garanteixi el millor rendiment d'acord amb els requisits establerts.

Competències transversals de la titulació.

- EPS6. Capacitat d'anàlisi i síntesi.

Competències estratègiques de la UdL.

- CT2. Adquirir un domini significatiu d'una llengua estrangera, especialment de l'anglès.

- CT3. Adquirir capacitat en l'ús de les noves tecnologies i de las tecnologies de la informació i la comunicació.

## Continguts fonamentals de l'assignatura

1. Sistemes d'equacions lineals.
  1. Formulació matricial.
  2. Mètode de Gauss.
  3. Factorització LU.
  4. Factorització QR.
  5. Norma d'una matriu.
  6. Valors i vectors propis de matrius quadrades.
  7. Mètodes iteratius.
  8. L'algoritme PageRank.
2. Transformacions geomètriques en el pla.
  1. Transformacions bàsiques.
  2. Representació matricial i coordenades homogènies.
  3. Transformacions inverses.
3. Interpolació polinòmica.
  1. L'anell de polinomis.
  2. L'algoritme d'Euclides per a polinomis.
  3. Interpolació polinòmica: el mètode de Lagrange.
  4. Esquemes per a compartir secrets: l'esquema de Shamir.
4. Aritmètica modular.
  1. Anells de classes de residus
  2. Cossos finits.
  3. Tests de primalitat.
  4. Algoritmes de factorització.
5. Introducció a la Criptografia.
  1. Criptosistemes simètrics.
  2. Criptosistemes de clau pública.
  3. El problema de la factorització d'enters.
  4. El criptosistema RSA.
  5. El problema del logaritme discret.
  6. El criptosistema ElGamal.
  7. Signatures digitals.
  8. Criptografia amb corbes el·líptiques.

## Eixos metodològics de l'assignatura

Se combinen classes de teoria, classes de problemes y classes 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.

## Pla de desenvolupament de l'assignatura

Setmana	Descripció	Activitat presencial	Treball autònom
1	Introducció. Sistemes d'equacions lineals.	Presentació de l'assignatura. 1.1, 1.2: Mètode de Gauss.	Estudiar la bibliografia i el pla de l'assignatura.
2	Sistemes d'equacions lineals.	1.3, 1.4: Descomposicions QR i LU.	Exercicis i resolució de problemes amb SAGE.

3	Sistemes d'equacions lineals.	1.5,1.6, 1.7: Mètodes iteratius.	L'algoritme Page Rank.
4	Transformacions geomètriques en el pla.	2.1: Transformacions bàsiques en el pla.	Exercicis i resolució de problemes amb SAGE.
5	Transformacions geomètriques en el pla.	2.2, 2.3: Formulació matricial i transformacions inverses.	Transformacions al pla en SAGE.
6	Interpolació polinòmica.	3.1, 3.2: Anells de polinomis. L'algoritme d'Euclides en anells de polinomis.	Exercicis i resolució de problemes amb SAGE.
7	Interpolació polinòmica.	3.3, 3.4: Interpolació. Interpolació de Lagrange. L'esquema de Shamir de compartició de secrets	Exercicis i resolució de problemes amb SAGE.
8	Aritmètica modular.	.4.1, 4.2: Anells de classes de residus, Cossos finits.	Exercicis i resolució de problemes amb SAGE.
9		<b>1er Examen Parcial</b>	Preparació examen.
10	Aritmètica modular.	4.3, 4.4: Primalitat i factorització.	Exercicis i resolució de problemes amb SAGE.
11	Introducció a la criptografia.	5.1,5.2: Nocions bàsiques de criptografia.	Exercicis i resolució de problemes amb SAGE.
12	Introducció a la criptografia.	5.3, 5.4: Factorització i RSA.	El criptosistema RSA amb SAGE.
13	Introducció a la criptografia.	5.5, 5.6: Logaritmes discrets i xifrat d'El Gamal.	El xifrat d'El Gamal amb SAGE.
14	Introducció a la criptografia.	5.7: Signatura Digital.	Exercicis i resolució de problemes amb SAGE.
15	Introducció a la criptografia.	5.8: Criptografia amb corbes el·líptiques.	Exercicis i resolució de problemes amb SAGE.
16		<b>2on Examen Parcial</b>	Preparació examen.
17		<b>2on Examen Parcial</b>	Preparació examen.
18		Exposicions orals.	Preparació de presentacions orals.
19		<b>Recuperació</b>	Preparació examen.

## Sistema d'avaluació

Abr.	Activitat d'avaluació	Ponderació	Nota mínima	En grup	Obligatòria	Recuperable
C1	Pràctica de SAGE	10%	NO	NO	SI	NO
P1	1er Examen Parcial	40%	1.5	NO	SI	SI
C2	Presentació oral	10%	NO	SI ( $\leq 2$ )	SI	NO
P2	2on Examen Parcial	40%	1.5	NO	SI	SI

PCL	Participació a classe	0,5 punts	NO	NO	NO	NO
Els exàmens parcials, la pràctica de SAGE i la presentació oral són obligatoris.						
<b>Nota Final</b> = $0,1 \cdot C1 + 0,4 \cdot P1 + 0,1 \cdot C2 + 0,4 \cdot P2 + 0,05 \cdot PCL$						

L'assignatura se supera si la nota final és igual a 5 o superior. La nota final és la suma ponderada dels exàmens parcials, la pràctica de SAGE, de la presentació oral i addicionalment d'un màxim de 0,5 punts de participació a classe i d'avaluació continuada. Els exàmens parcials són per escrit, tenen un pes del 40% sobre la nota final cadascun d'ells i tenen una nota mínima de 1,5 punts per a ser avaluables. Els exàmens parcials, la pràctica de SAGE i la presentació oral són obligatoris. Es poden obtenir fins a 0,5 punts addicionals per una participació activa a classe i per altres activitats d'avaluació continuada que seran degudament anunciats. L'examen de recuperació consta del 1er o del 2on parcial o de tots dos, a criteri de l'estudiant.

## Bibliografia i recursos d'informació

- 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.