



Universitat de Lleida

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

Any acadèmic 2013-14

## Informació general de l'assignatura

<b>Denominació</b>	EINES COMPUTACIONALS PER A LA RESOLUCIO DE PROBLEMES
<b>Codi</b>	102042
<b>Semestre d'impartició</b>	7è Q Avaluació Continuada
<b>Caràcter</b>	Obligatòria
<b>Nombre de crèdits ECTS</b>	6
<b>Grups</b>	1
<b>Crèdits teòrics</b>	0
<b>Crèdits pràctics</b>	0
<b>Departament/s</b>	Matemàtica
<b>Distribució càrrega docent entre la classe presencial i el treball autònom de l'estudiant</b>	1,5 de treball autònom per cada hora de treball presencial
<b>Informació important sobre tractament de dades</b>	Consulteu <a href="#">aquest enllaç</a> per a més informació.
<b>Idioma/es d'impartició</b>	Anglès
<b>Distribució de crèdits</b>	Josep M. Miret Biosca 3 Jordi Pujolàs Boix 3
<b>Horari de tutoria/lloc</b>	Concertar cita per correu electrònic

Josep M. Miret Biosca  
Jordi Pujolàs Boix

## Competències

Capacitat per comprendre i dominar els conceptes fonamentals d'àlgebra compuacional i teoria de nombres, i la seva aplicació per a la resolució de problemes propis de l'enginyeria.

Capacitat per a la resolució dels problemes computacionals que puguin plantejar-se en l'enginyeria.

Capacitat per adquirir destresa en l'ús de software matemàtic.

## Continguts fonamentals de l'assignatura

### 1. Vector spaces.

- *Vector spaces: definition and examples.*
- *Basis of a vector space.*
- *Linear applications*
- *Matrix associated to a linear application*
- *Endomorphisms*
- *Eigenvalues and eigenvectors*
- *Diagonalization of an endomorphism*
- *PageRank algorithm*

### 2. Systems of linear equations.

- *Matrix formulation.*
- *Gauss' method.*
- *Factorization LU.*
- *Factorization QR.*
- *Norm of a matrix.*
- *Iterative methods.*

### 3. Polynomials.

- *The ring of polynomials.*
- *Roots of a polynomial.*
- *Euclid's algorithm for polynomials.*
- *Irreducible polynomials.*
- *Polynomial decomposition.*
- *Polynomial interpolation.*
- *Secret sharing schemes: Shamir's scheme*

## 4. Primes.

- *How many primes are there?*
- *Primality tests.*
- *Distribution of primes.*
- *Factorization algorithms.*

## 5. Finite fields.

- *Prime finite fields.*
- *Construction of finite fields.*
- *Representation of elements.*

## 6. Applications to Cryptography.

- *Symmetric cryptosystems.*
- *Public key cryptosystems.*
- *Integer Factorization Problem.*
- *RSA cryptosystem.*
- *Discrete Logarithm Problem.*
- *ElGamal cryptosystem.*
- *Digital signatures.*
- *Elliptic Curve Cryptography.*

## Eixos metodològics de l'assignatura

Es combinen classes de teoria, classes de problemes i classes amb el programari de càlcul simbòlic SAGE. Les classes de teoria aporten els conceptes bàsics de l'assignatura, tot incorporant exemples il·lustratius que en faciliten la comprensió. En les classes de problemes es combinen la resolució conjunta a la pissarra, amb la resolució individual i en grup dels estudiants en la mateixa aula.

## Sistema d'avaluació

L'avaluació es basarà en els següents ítems:

- \* prova escrita dels temes 1,2,3 (4 punts)
- \* prova escrita dels temes 4,5,6 (4 punts)
- \* pràctica en SAGE (1 punt)
- \* presentació oral d'un treball (1 punt)

En cadascuna de les proves de 4 punts cal treure com a mínim 1.5 punts

Es podran recuperar una o les dues proves escrites durant la setmana de recuperacions.

Es pot obtenir 0.5 punts addicionals per la participació a classe.

## 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.