DEGREE CURRICULUM

EINES COMPUTACIONALS PER A LA RESOLUCIO DE PROBLEMES

Academic year 2013-14

COMPUTATIONAL TOOLS FOR PROBLEM SOLVING 2013-14

Subject's general information

Subject name	EINES COMPUTACIONALS PER A LA RESOLUCIO DE PROBLEMES
Code	102042
Semester	7è Q Avaluació Continuada
Typology	Obligatòria
ECTS credits	6
Groups	1
Theoretical credits	0
Practical credits	0
Department	Matemàtica
Teaching load distribution between lectures and independent student work	1,5 de treball autònom per cada hora de treball presencial
Important information on data processing	Consult this link for more information.
Language	Anglès
Distribution of credits	Josep M. Miret Biosca 3 Jordi Pujolàs Boix 3
Office and hour of attention	Concertar cita per correu electrònic

COMPUTATIONAL TOOLS FOR PROBLEM SOLVING 2013-14

Josep M. Miret Biosca
Jordi Pujolàs Boix

Competences

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.

Subject contents

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 descomposition.*
    - *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.*

Methodology

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.

Evaluation

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.

Bibliography

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.