DEGREE CURRICULUM

COMPUTATIONAL TOOLS FOR PROBLEM SOLVING

Coordination: PUJOLAS BOIX, JORDI

Academic year 2019-20

COMPUTATIONAL TOOLS FOR PROBLEM SOLVING 2019-20

Subject's general information

<table>
<tr><td>Subject name</td><td>COMPUTATIONAL TOOLS FOR PROBLEM SOLVING</td></tr>
<tr><td>Code</td><td>102042</td></tr>
<tr><td>Semester</td><td>1st Q(SEMESTER) CONTINUED EVALUATION</td></tr>
<tr><td>Typology</td><td>
<table>
<tr><th>Degree</th><th>Course</th><th>Character</th><th>Modality</th></tr>
<tr><td>Bachelor's Degree in Computer Engineering</td><td>4</td><td>COMPULSORY</td><td>Attendance-based</td></tr>
</table>
</td></tr>
<tr><td>Course number of credits (ECTS)</td><td>6</td></tr>
<tr><td>Type of activity, credits, and groups</td><td>
<table>
<tr><th>Activity type</th><th>PRAULA</th><th>TEORIA</th></tr>
<tr><td>Number of credits</td><td>3</td><td>3</td></tr>
<tr><td>Number of groups</td><td>1</td><td>1</td></tr>
</table>
</td></tr>
<tr><td>Coordination</td><td>PUJOLAS BOIX, JORDI</td></tr>
<tr><td>Department</td><td>MATHEMATICS</td></tr>
<tr><td>Teaching load distribution between lectures and independent student work</td><td>150 total hours of work
60 hours lecture attendance
90 hours student work</td></tr>
<tr><td>Important information on data processing</td><td>Consult this link for more information.</td></tr>
<tr><td>Language</td><td>English</td></tr>
<tr><td>Distribution of credits</td><td>Josep M. Miret Biosca 3
Jordi Pujolàs Boix 3</td></tr>
<tr><td>Office and hour of attention</td><td>Appointment by email.</td></tr>
</table>

COMPUTATIONAL TOOLS FOR PROBLEM SOLVING 2019-20

Teaching staff	E-mail addresses	Credits taught by teacher	Office and hour of attention
ADJ , GORA	gora.adj@udl.cat	3,2	
PUJOLAS BOIX, JORDI	jordi.pujolas@udl.cat	4	

Subject's extra information

Requirements: Algebra, Statistics and Optimization, Introduction to Programming 1.

Learning objectives

The learning outcomes that the student must achieve in this subject are:

- To solve systems of linear equations by different direct methods: Gauss, LU and QR.
- To determine the eigenvalues and eigenvectors of a square matrix.
- To solve systems of linear equations by iterative methods and to know their convergence conditions.
- To know and use the most common geometric transformations in the plane to move objects.
- To determine the interpolation polynomial of a set of points in the plane.
- To distribute shares of a key using Shamir's secret sharing scheme.
- To know and properly use factoring algorithms and primality tests.
- To encrypt, decrypt and digitally sign using RSA and ElGamal cryptosystems.
- To acquire computer skills to solve mathematical problems using SAGE software.

Competences

Specific competences of the degree.

- GII-C1. Capacity to have a deep knowledge of the basic principles and models for computation and to know how to apply them in order to interpret, select, value, model, and create new concepts, theories, uses and technological developments related with the informatics.
- GII-C3. Capacity to evaluate the computational complexity of a problem, to know the algorithmic strategies that can drive to its solving and recommend, develop and implement the one which guarantee the best performance in accordance with the requirements.

Cross-disciplinary competences of the degree.

- EPS6. Capacity to work in situations with a lack of information and/or under pressure.

Strategic competences of the UdL.

- CT2. Mastering a foreign language, especially English.
- CT3. Training Experience in the use of the new technologies and the information and communication technologies.

Subject contents

1. Finite fields
    1. Rings of integers modulo n
    2. Prime numbers
    3. Prime finite fields
    4. Binary fields
    5. Constructing finite fields
    6. Representing the elements
2. Cryptography
    1. Symmetric cryptosystems
    2. Public key cryptosystems
    3. Integer factorization problem
    4. RSA cryptosystem
    5. Discrete Logarithm Problem
    6. ElGamal cryptosystem
    7. Digital signatures
    8. Elliptic Curve Cryptography
3. Secret sharing schemes
    1. The polynomial ring
    2. Polynomial interpolation: Lagrange's method
    3. Secret sharing schemes: Shamir's scheme
4. PageRank algorithm
    1. Systems of linear equations
    2. Iterative methods
    3. Eigenvalues and eigenvectors
    4. Diagonalization of a square matrix
    5. The power method
    6. Application to the PageRank problem
5. Geometric transformations of the plane
    1. Basic transformations
    2. Matrix representation and homogeneous coordinates
    3. Inverse transformations
6. Error detection and correction codes
    1. Information transmission
    2. Information codification
    3. Error correcting codes

Methodology

Theoretical and practical contents are mixed to combine basic aspects with illustrative examples and problem solving. Practical lectures include sessions with the open symbolic package SAGE.

Development plan

Week	Description	Classroom Activity	Autonomous work
1	Introduction Systems of linear equations.	Introducting Lecture 1.1, 1.2: Gauss' method.	Study bibliography and plan.

2	Systems of linear equations.	1.3, 1.4: QR and LU decompositions.	Exercises and problem solving with SAGE
3	Systems of linear equations.	1.5,1.6, 1.7: Iterative methods.	Page Rank Algorithm implementation.
4	Geometric transformations of the plane.	2.1: Basic transformations.	Exercises and problem solving with SAGE
5	Geometric transformations of the plane.	2.2, 2.3: Matrix formulation and inverse transformations.	Geometric transformations in SAGE.
6	Polynomial interpolation.	3.1, 3.2: Polynomial rings. The Euclidean Algorithm for polynomials.	Exercises and problem solving with SAGE.
7	Polynomial interpolation.	3.3, 3.4: Interpolation. Lagrange interpolation. Shamir's secret sharing scheme.	Exercises and problem solving with SAGE. Shamir's scheme in SAGE.
8	Modular arithmetic	4.1, 4.2: Remainder class rings. Finite fields.	Exercises and problem solving with SAGE.
9		**1st Partial Exam**	Exam preparation.
10	Modular arithmetic	4.3, 4.4: Primality and factorization.	Exercises and problem solving with SAGE.
11	Introduction to Cryptography.	5.1,5.2: Basic notions.	Exercises and problem solving with SAGE.
12	Introduction to Cryptography.	5.3, 5.4: Factorization and RSA.	Exercises and problem solving with SAGE. RSA cryptosystem in SAGE.
13	Introduction to Cryptography.	5.5, 5.6: Discrete logs and El Gamal encryption.	El Gamal encryption in SAGE.
14	Introduction to Cryptography.	5.7: Digital Signatures.	Exercises and problem solving with SAGE.
15	Introduction to Cryptography.	5.8 Elliptic curve cryptography.	Exercises and problem solving with SAGE.
16		**2nd Partial Exam**	Exam preparation
17		**2nd Partial Exam**	Exam preparation
18			Short talks.
19		**2nd chance Exam**	Exam preparation

Evaluation

Abbr.	Marking Activity	Ponderation	Minimum Mark	Group	Compulsory	Mendable
C1	SAGE Test	10%	NO	NO	YES	NO
P1	1st Partial Exam	40%	1.5	NO	YES	YES

C2	Oral presentation	10%	NO	YES (<=2)	YES	NO
P2	2nd Partial Exam	40%	1.5	NO	YES	YES
PCL	Classroom participation	0.5 points	NO	NO	NO	NO
Both partial exams, the SAGE activity and the oral presentation are compulsory.						
Final Mark = 0.1*C1 + 0.4*P1 + 0.1*C2 + 0.4*P2 + 0.05*PCL						

The course is passed if the final mark is 5 or higher. The final mark is a weighted sum of both partial exams, the SAGE coding exercise and the short oral presentation plus a maximum 0.5 points due to classroom participation. Each partial exam is a written exam and has a weight of 40% in the final mark, with a minimum mark of 1.5 required. Both partial exams, the SAGE test and the short oral presentation are compulsory. One or both written partial exams are eligible for second chance examination. An extra 0.5 points is obtainable for class participation.

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.