DEGREE CURRICULUM

MATHEMATICS FOR COMPUTING

Coordination: DALFÓ SIMÓ, CRISTINA

Academic year 2019-20

Subject's general information

Subject name	MATHEMATICS FOR COMPUTING
Code	102372
Semester	1st Q(SEMESTER) CONTINUED EVALUATION
Typology	<table><tr><th>Degree</th><th>Course</th><th>Character</th><th>Modality</th></tr><tr><td>Bachelor's degree in Digital Interaction and Computing Techniques</td><td>1</td><td>COMMON</td><td>Attendance-based</td></tr></table>
Course number of credits (ECTS)	6
Type of activity, credits, and groups	<table><tr><th>Activity type</th><th>PRAULA</th><th>TEORIA</th></tr><tr><th>Number of credits</th><td>3</td><td>3</td></tr><tr><th>Number of groups</th><td>1</td><td>1</td></tr></table>
Coordination	DALFÓ SIMÓ, CRISTINA
Department	MATHEMATICS
Teaching load distribution between lectures and independent student work	6 ECTS correspond to a workload of 60 h of lectures and assessment and 90 h autonomous study work for each student.
Important information on data processing	Consult this link for more information.
Language	Catalan
Distribution of credits	3 theoretical credits and 3 practical credits

Teaching staff	E-mail addresses	Credits taught by teacher	Office and hour of attention
DALFÓ SIMÓ, CRISTINA	cristina.dalfo@udl.cat	6	

Subject's extra information

Previous knowledge/skills in basic mathematics (General Upper Secondary Education level) are recommended.
This subject is scheduled in the fall semester of the 1st year.
The knowledge and competencies acquired in this subject will be useful to follow other subjects with contents related to logic, data structure, discrete mathematics and other subjects in Computation.

Learning objectives

- Appropiately use set operations, both to simplify expressions or to prove equalities.

- Distinguish injective, exhaustive and bijective maps.

- Manipulate the composition of maps and inverse maps.

- Appropiately use matrix operations and solve systems of linear equations.

- Apply mathematical induction to show different mathematical statements.

- Recognize the algebraic structures of group, ring and field.

- Adequately use the elements in modular arithmetic.

- Solve diophantine equations and linear congruencies.

- Encrypt and decrypt with the RSA cryptosystem.

Competences

Specific competences:

CE1. Capacity to formalise and solve computational problems, by using the mathematical language from the algebra and set theory.

CE2. Capacity to understand and master the basic concepts of discreet mathematics, logical, algorithmic and computational complexity, and its application to solve computational problems.

Cross-disciplinary competences:

CT5. Acquire knowledge in scientific thinking.

Subject contents

I. SET THEORY

1. Sets.

- Sets and elements. Subsets.

- Set operations.

- Laws of the algebra of sets.

- Partition of a set.

- Cartesian product.

2. Maps.

- Map between sets: definitions and examples.

- Injective, surjective and bijective maps.

- Composition of maps.

- Inverse map.

3. Matrix theory, determinants and systems of linear equations.

- Matrix operations.

- Invertible matrices.

- Equivalent matrices and rank of a matrix.

- Determinants: definition, properties and effective computation.

- Systems of linear equations: matrix formulation.

- Rouché-Frobenius Theorem.

- Gauss method.

4.Induction and denumerability

- Mathematical induction.

- Infinite sets and denumerable sets.

II. ALGEBRAIC STRUCTURES AND ARITHMETIC

5. Algebraic structures.

- Algebraic composition laws. Properties.

- Group structure: definitions, properties, examples.

- Ring and field structures: definitions, properties, examples.

6. Modular arithmetic.

- Division of integers. Divisors and multiples.

- Greatest Common Divisor. Euclidean algorithm. Bézout's identity.

- Linear diophantine equations.

- Prime numbers. Fundamental theorem of arithmetic.

- Congruences. Linear congruences.

- Chinese remainder theorem.

- Modular exponentiantion. Fermat's and Euler's Theorems.

- Introduction to cryptography: RSA cryptosystem.

Methodology

Theoretical and practical contents are mixed for the sake of combining basical aspects with illustrative examples and problem solving.

Problem solving combines joint resolution on the blackboard or individual resolution. Some sessions will be devoted to group problem solving. Proposed problems are either solved and presented by students, or collected to be assessed.

The students will be provided beforehand with the collection of problems to be solved, as well as the exams of previous years, which will be solved in groups.

Development plan

Week	Lesson	Activities	Study workload
1	Introduction. Lesson 1	Lectures	4 hours. Study and problem solving
2	Lesson 1	Lectures and problem sessions	4 hours. Study and problem solving
3	Lesson 1	Lectures and problem sessions	4 hours. Study and problem solving
4	Lesson 2	Lectures and problem sessions	4 hours. Study and problem solving
5	Lesson 2	Control 1	6 hours. Study for control
6	Lesson 3	Lectures and problem sessions	4 hours. Study and problem solving
7	Lesson 3	Lectures and problem sessions	4 hours. Study and problem solving
8	Lesson 4	Lectures and problem sessions	6 hours. Study and problem solving
9		Partial 1 Assessment	6 hours. Study for exam
10	Lesson 4	Lectures and problem sessions	4 hours. Study and problem solving
11	Lesson 5	Control 2	6 hours. Study for control
12	Lesson 5	Lectures and problem sessions	4 hours. Study and problem solving
13	Lesson 6	Lectures and problem sessions	4 hours. Study and problem solving
14	Lesson 6	Lectures and problem sessions	4 hours. Study and problem solving
15	Lesson 6	Lectures and problem sessions	8 hours. Study for exam
16		Tutorization	8 hours. Study for exam
17		Partial 2 Assessment	8 hours. Study for exam
18		Tutorization	
19		Final Assessment	

Evaluation

Acr.	Assessment Activities	Weight	Minimum Mark	Reevaluation

C1	Control 1 (Lesson 1)	10%	No	No
P1	Partial 1 (Lessons 1, 2, 3)	40%	2.5 points (over 10)	Yes
C2	Control 2 (Lesson 4)	10%	No	No
P2	Partial 2 (Lessons 4, 5, 6)	40%	2.5 points (over 10)	Yes
AC	Complementary activity	0.5 extra points (over 10)	No	No
PCl	Participation	0.5 extra points (over 10)	No	No

A student with a final mark below 5 or who has not reached the minimum marks required, can reevaluate either P1, P2 or both.

Final Mark = C1 + P1 + C2 + P2 + AC+ PCL

Bibliography

Books including problems:

- ALSINA, M; BUSQUÉ, C; VENTURA, E. Problemes d'Àlgebra. Servei de Publicacions de l'U.A.B., 1990.
- BIJEDIC, N; GIMBERT, J; MIRET,J.M; VALLS, M. Elements of Discrete Mathematical Structures for Computer Science. Univerzittska knjiga Mostar, 2007.
- ESPADA, E. Problemas resueltos de Álgebra (Vol I,II). EDUNSA, 1989.
- GIMBERT, J; HERNÁNDEZ, X; LÓPEZ, N; MIRET, J.M; MORENO, R; VALLS, M. Curs Pràctic d'Àlgebra per a Informàtics, Col.lecció Eines. Edicions de la Universitat de Lleida, 2004.

Theory books:

- ANTON, H. Introducción al Álgebra Lineal. Ed. Limusa, 3a. edició, 1990.
- CASTELLET, M; LLERENA, I. Àlgebra Lineal i Geometria. Manuals de la Universitat Autònomade Barcelona, 1979.
- CHILDS, L. A Concrete Introduction to Higher Algebra. Springer, 1a. edició, 1979.
- STANAT, D.F.; McALLISTER, D.F. Discrete Mathematics in Computer Science, Prentice-Hall, 1a. Edició.

Recommended reading:

SINGH, S. The Code Book: The Secret History of Codes and Code-breaking, HarperCollins Publishers, London, 1999.

There are the original English version in paper and also the ebook.

There is the Spanish version in paper: SINGH, S. Los códigos secretos. Ed. Debate, 2000.