Teaching Guide					
Identifying Data					2018/19
Subject (*)	Algebra			Code	614G01010
Study programme	Grao en Enxeñaría Informática				
Descriptors					
Cycle	Period	Year		Type	Credits
Graduate	2nd four-month period	First		Basic training	6
Language	SpanishGalicianEnglish				
Teaching method	Face-to-face				
Prerequisites					
Department	Computación				
Coordinador	Vieites Rodriguez, Ana Maria		E-mail	ana.vieites@udc.es	
Lecturers	Aguado Martin, Maria Felicidad Barja Pérez, José María Costoya Ramos, Maria Cristina Doncel Juarez, Jose Luis Perez Vega, Gilberto Souto Salorio, Maria Jose Vidal Martin, Concepcion Vieites Rodriguez, Ana Maria		E-mail	felicidad.aguado@udc.es j.m.barja@udc.es cristina.costoya@udc.es jose.luis.doncel@udc.es gilberto.pvega@udc.es maria.souto.salorio@udc.es concepcion.vidalm@udc.es ana.vieites@udc.es	
Web	campusvirtual.udc.es/moodle				
General description	This course is part of the basic training module in the Computer Engineering degree. It is intended for acquiring skills in formal and abstract thinking, which will be essential in the performance of the students future professions. The main purpose of this subject is to introduce the basic notions of modular arithmetic, matrix theory and linear algebra. Emphasis is given to topics that will be useful in other subjects: Computer Security, Computer Graphics, Artificial Vision, Digital Image Processing, and Networks. We are concerned with an algorithmic approach emerging from the interplay of Algebra and Computer Engineering. In this course, students will learn how to design and analyze efficient algorithms for elementary number theory and linear algebra.				

Study programme competences	
Code	Study programme competences
A1	Capacidade para a resolución dos problemas matemáticos que se poden presentar na enxeñaría. Aptitude para aplicar os coñecementos sobre: álxebra linear; cálculo diferencial e integral; métodos numéricos; algorítmica numérica; estatística e optimización.
A3	Capacidade para comprender e dominar os conceptos básicos de matemática discreta, lóxica, algorítmica e complexidade computacional e a súa aplicación para a resolución de problemas propios da enxeñaría.
B3	Capacidade de análise e síntese
B6	Toma de decisións
C1	Expresarse correctamente, tanto de forma oral coma escrita, nas linguas oficiais da comunidade autónoma.
C6	Valorar criticamente o coñecemento, a tecnoloxía e a información dispoñible para resolver os problemas cos que deben enfrontarse.
C7	Asumir como profesional e cidadán a importancia da aprendizaxe ao longo da vida.

Learning outcomes			
Learning outcomes	Study programme competences		
Acquire basic concepts from Elementary Number Theory.	A1 A3		

Interpret and apply the acquired knowledge from Elementary Number Theory to Cryptography.	A1 A3	B3	
Know some basic concepts of Linear Algebra: systems of linear equations, vectorial spaces, matrices and linear maps.	A1		
Use Linear Algebra as a tool for modeling and solving processes related to computer science.	A1	B6	C6
Know the definitions and basic principles from Coding Theory related to Linear Algebra.	A1		
Simulate coding and decoding processes using matricial techniques.	A1	B6	C6
Learn how to use mathematical language in a proper way to express ideas.	A1		C1
Develop the capacities of abstraction, concretion, concision, imagination, intuition, reasoning, criticism, objectivity, synthesis and accuracy; put all of them in practice either in the academic or the professional life for solving problems successfully.		B3	C7
Apply basic concepts from the subject and relate to algorithmic and computational concepts in the light of the mathematical ones.	A1		C6
Acquire tools and skills for solving problems in a proper way. Express and interprete results in a rigorous way. Check the result and, in case of any incongruence, revise the process to detect the error.	A1	B6	C1 C7

Contents	
Topic	**Sub-topic**
Chapter 1: Modular arithmetic: application to Cryptography.	Basic concepts from elementary number theory. Euclides' algorithm. Prime numbers. Linear diophantine equations. Congruences. Modular arithmetic. Definition of cryptosystem. Classical cryptography. Symmetrical and asymmetrical cryptography. Examples of cryptosystems. Numeration systems. Divisibility criteria.
Chapter 2: Systems of Linear Equations, Matrices and Determinants.	Definition and properties of systems of linear equations. Echelon row form of system. Gauss method. Matrices. Operations with matrices. Invertible matrix. Determinant of a square matrix, properties. Cramer's rule.
Chapter 3: Vector Spaces.	Definition and properties of a vector space. Bases and coordinates. Dimension. Rank of a set of vectors and matrix rank. Computation of the rank. Change of basis. Rouché-Frobenius theorem.
Chapter 4. Linear maps.	Definición e propiedades das aplicacions lineais. Núcleo e imaxe de unha aplicación lineal. Matriz asociada a unha aplicación lineal. Teorema da dimensión. Definition and properties of linear maps. Kernel and image of a linear map. Matrix associated to a linear map. Dimension theorem.
Chapter 5. Linear Codes	Definition of linear codes. Parameters of a linear code. Hamming distance and Hamming weight. Generator matrix and parity-check matrix of a code. Error correction in linear codes. Binary Hamming codes.

Planning				
Methodologies / tests	**Competencies**	**Ordinary class hours**	**Student?s personal work hours**	**Total hours**
Guest lecture / keynote speech	A1 A3 C6 C7	30	37.5	67.5
Laboratory practice	A1 B3 B6 C1 C6	20	30	50
Collaborative learning	A1 B3 C1 C7	10	17.5	27.5
Personalized attention		5	0	5
(*)The information in the planning table is for guidance only and does not take into account the heterogeneity of the students.				

Methodologies	
Methodologies	**Description**

Guest lecture / keynote speech	The chief means of communication for this course will be the platform Moodle. Students are expected to check this for up-to-date assignments-including material separate from the given at the blackboard-and announcements. Over the semester we will study many topics that form a central part of the language of modern science. Weekly problem sets with a mix of exercices will be given. These include problems requiring abstraction, understanding and/or synthesis of various concepts. In many ways, these constitue the heart of the course; rigor in their completion often yields the greatest understanding. We want the student to leave the course not only with computational ability, but with the ability to use these notions in their natural scientific contexts, and with an appreciation of their mathematical power.
Laboratory practice	The laboratory work is the focal point of learning. A series of exercises related to the theoretical contents explained in the theoretical classes will be given to students at the beginning of every chapter. It ensures that: I) students work closely with the teacher helping them to grow in confidence, to develop their skills in analysis, and to encourage them to reinforce the learning of theoretical concepts through the resolution of the exercises. II) students gain capacity of abstraction and understanding. A typical laboratory practice is a 2-hour class, with small groups of students, discussing the resolution of the exercises. It gives students the chance to interact directly with teachers, to exchange ideas and argue between them, to ask questions, and of course, to learn through the discussion. Technology can play an important role in the learning of mathematics, and as such, graphing and scientific calculators are permitted for class and homework, though they will not be permitted on tests and quizzes, and thus it is emphasized that students learn not to rely on them. Subject to availability, some exercises may be designed to be solved with computers.
Collaborative learning	Collaboration is encouraged, for home and class assignments; however, all submitted assignments must be written up independently and represent the student?s own work and understanding.

Personalized attention	
Methodologies	**Description**
Guest lecture / keynote speech Laboratory practice Collaborative learning	The studens have the possibility to revise the qualification obtained in the written final test, proving that this is adjusted to the criteria of evaluation established. Likewise, the evaluations of the answers to the questions and exercises formulated during the course, with the indications adequate in order to correct the errors and/or improve the answers with a view to a more solid formation, will justify. In the sessions in reduced groups, the doubts formulated by the students are solved in an individualized way, especially when they are common to several of them or illustrate an interesting case. If the question is more particular or does completely not remain solved for some pupil, it would be treated in the hours of individualized tuition. Students registered to partial time: Depending on the particularities of every specific case and the possibilities of the teaching staff put in charge of the group to the that it is a pupil registered in time partial assigned, the tests of the continuous evaluation will be adjusted so that this pupil can obtain the same qualification as a pupil of ordinary registration.

Assessment

Methodologies	Competencies	Description	Qualification
Guest lecture / keynote speech	A1 A3 C6 C7	At the end of the course a written test will be carried out. This test includes a maximum of 8 questions. Among them, you will find: - Short questions of basic theoretical concepts. - Exercises with a degree of difficulty that is similar to exercises solved during the semester. As well as demonstrating skill in the appropriate techniques, candidates will be expected to apply knowledge in the solution of problems. Candidates will also be expected to write with clarity, taking care of the presentation. With the final test, the student ends the process of continuous evaluation. To add the practical note to the exam note it is necessary to obtain more than three points of the eight possible ones in the final exam.	80
Laboratory practice	A1 B3 B6 C1 C6	This section will consist of, at least, 2 structured or problem-solving questions based on the different topics, similar to exercises from the weekly 2-hour session classes. Correct answers as well as the presentation and clarity of the exposition will be valued. A participative attitude of the student in the resolution of the proposed exercises during the sessions will also be positively valued.	20
Collaborative learning	A1 B3 C1 C7	An active participation of the students will be positively valued.	0
Others			

Assessment comments
Evaluation of the student registered in time partial: Depending on the particularities of every specific case and the possibilities of the teaching staff put in charge of the group to the that it is a student registered in time partial assigned, the tests of the continuous evaluation will be adjusted so that this student can obtain the same qualification as a student of ordinary registration.In the opportunity advanced to December, the examination will be qualified on ten points, being necessary to obtain at least one five to approve the matter.

Sources of information	
Basic	- Grossman, S. I. (1996). Álgebra lineal con aplicaciones. McGraw-Hill Interamericana México. - Grossman, S. I. (1994). Elementary Linear Algebra with Applications. Wiley - Merino, L. y Santos, E. (2006). Álgebra Lineal con Métodos Elementales. Thomson. - Cameron, P. J. (1998). Introduction to Algebra. Oxford University Press, Oxford. - Rosen, K. H. (2004). Matemática Discreta y sus aplicaciones. McGraw-Hill Interamericana. - Rosen, K. H. (2003). Discrete Mathematics and Its Applications. McGraw-Hill - Biggs, N. L. (1994). Matemática Discreta. Madrid, Vicens Vives. - Lay, D. C. (2011). Linear Algebra and Its Applications. Pearson - Lay, D. C. (2007). Algebra Lineal y sus Aplicaciones. Prentice Hall

Complementary	- Hernández, E. (1994). Álgebra y Geometría. Addison-Wesley. - Rojo, J. y Martín, I. (2005). Ejercicios y problemas de Álgebra Lineal. McGraw-Hill. - Lidl, R. y Pilz, G. (1998). Applied Abstract Algebra. Nueva York, Springer. - Torrecilla Jover, B. (1999). Fermat. El Mago de los Números. Nivola. - Van Lint, J. H. (1999). Introduction to Coding Theory. Berlín, Springer. - Singh, S. (2000). Los Códigos Secretos. Debate - Nakos, G. y Joyner, D. (1999). Álgebra lineal con aplicaciones. Thomson. - Nakos, G. y Joyner, D. (1998). Linear Algebra with Applications. Brooks Cole Publising

Recommendations
Subjects that it is recommended to have taken before
Discrete Mathematics/614G01004
Subjects that are recommended to be taken simultaneously
Subjects that continue the syllabus
Other comments

(*)The teaching guide is the document in which the URV publishes the information about all its courses. It is a public document and cannot be modified. Only in exceptional cases can it be revised by the competent agent or duly revised so that it is in line with current legislation.