Teaching Guide				
Identifying Data				2015/16
Subject (*)	Algebra		Code	614G01010
Study programme	Grao en Enxeñaría Informática			
Descriptors				
Cycle	Period	Year	Type	Credits
Graduate	2nd four-month period	First	FB	6
Language	SpanishGalicianEnglish			
Teaching method	Face-to-face			
Prerequisites				
Department	Computación			
Coordinador	Doncel Juarez, Jose Luis	E-mail	jose.luis.doncel@udc.es	
Lecturers	Aguado Martin, Maria Felicidad Barja Pérez, José María Blanco Ferro, Antonio angel 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 antonio.blanco.ferro@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 methods from 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 that are 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 facing and 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
Adquirir ferramentas e destrezas para resolver os problemas de forma axeitada. Expresar e interpretar de forma precisa os resultados obtidos. Verificar o resultado e, en caso de obter unha incongruencia, revisar o proceso para detectar o erro cometido. 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 an 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	Across the virtual platform of the university, will put itself the arrangement of the student body the detailed information of the contents of every subject in order to that every pupil/to is configured, according to his criterion and needs, the material adequate for the follow-up and understanding of the matter, for that will be able to make use of the recommended bibliography and/or available material in the net. The theoretical and practical classes will keep coping in a simultaneous way in the classroom, carrying out exercises after the theoretical explanations, to a rhythm adequate for the total understanding of the ones constrained in order to achieve the suggested goals. A presentation of the formal techniques will be looked for by examples, with emphases in specific calculations and in the algorithmic nature of some of them. It will be intended that the pupils are capable of obtaining conclusions of the result incubated, attempting to motivate to the pupils so that they take part and they are capable of inferring conclusions that can be more or less evident.
Laboratory practice	A bulletin of exercises related to the theoretical contents explained in the classes of theory will facilitate it itself the pupils to the beginning of every subject. In these sessions it is aimed for: I) encouraging the pupil through the resolution of exercises, with the help of the professor, to reinforce the understanding of the incubated concepts, II) to encourage the resolution reasoned of the exercises, preventing the use of "recipes". Depending on the subject and on the available resources, works will be formulated with computer programs that reinforce the concepts worked in theoretical classes and of exercises. Together with the bulletin of exercises the goals or results of learning that they must obtain when finishing the subject will be indicated to the students.
Collaborative learning	Throughout the course they will dedicate themselves ten hours approximately so that the pupils formulate the doubts on the concepts, exercises and procedures seen in the sessions of theory and problems. Likewise small projects or the resolution of exercises in reduced groups of pupils can be formulated.

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	Ao final do curso realizarase unha proba escrita. Esta proba inclúe: - Preguntas curtas que permitan valorar se o alumno comprendeu os conceptos teóricos básicos. - Exercicios cun grao de dificultade similar aos realizados en clase e aos presentados nas coleccións de exercicios propostos. Avaliarase o dominio dos conceptos teóricos da materia, a comprensión destes e a súa aplicación na resolución de exercicios. Así mesmo, valorarase a claridade, a orde e a presentación dos resultados expostos. A presentación á proba final do curso supón que o estudante completou o proceso de avaliación continua. Para aprobar a materia é necesario obter máis de tres puntos dos oito posibles na proba escrita. At the end of the course a written test will be carried out. This test includes: - Short questions which they allow valuing if the pupil understood the basic theoretical concepts. - Exercises with a degree of difficulty similar to the ones carried out in class and to the ones presented in the collections of suggested exercises. The domination of the theoretical concepts of the matter, the understanding of these and his application in the resolution of exercises will be evaluated. Likewise, it will value itself the clarity, the order and the presentation of the exposed results. The presentation to the final test of the course means that the student completed the process of continuous evaluation. To approve the matter it is necessary to obtain more than three points of the eight possible ones in the written test.	80
Laboratory practice	A1 B3 B6 C1 C6	Ao longo do curso realizarase unha avaliación dos distintos temas onde se formularán preguntas sobre as definicións dos conceptos introducidos, cuestións e exercicios similares aos do correspondente boletín. Valorarase a resposta correcta ás cuestións e exercicios formulados así como a presentación e claridade da exposición realizada. Poderase valorar unha actitude participativa do alumnado na resolución das cuestións formuladas durante as prácticas e nas titorías en grupo reducido. A nota obtida neste apartado será a mesma nas dúas oportunidades da convocatoria do curso académico. Throughout the course an evaluation of the different subjects where questions will be formulated on the definitions of the introduced concepts, questions and exercises similar to those of the corresponding bulletin will be carried out. It will value itself the correct answer to the questions and formulated exercises as well as the presentation and clarity of the exhibition carried out. A participative attitude of the student body will be able to be valued in the resolution of the questions formulated during the practices and in the tuitions in reduced group. The note obtained in this section will be it in the two opportunities of the call of the academic course.	20
Collaborative learning	A1 B3 C1 C7	Valorarase a participación activa do alumnado nas sesións. The active participation of the student body will be valued in the sessions.	0
Others			

Assessment comments
Avaliación do alumnado matriculado a tempo parcial: Dependendo das particularidades de cada caso concreto e as posibilidades do profesorado encargado do grupo ao que estea asignado un estudante matriculado a tempo parcial, axustaranse as probas da avaliación continua para que o devandito estudante poida obter a mesma cualificación que un estudante de matrícula ordinaria.Na oportunidade adiantada a decembro, o exame cualificarase sobre dez puntos, sendo necesario obter polo menos un cinco para aprobar a materia.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.