UNIVERSIDAD DE
MURCIA

FACULTY OF
MATHEMATICS

Number Theory

Syllabus

Course code:	6362
Number of ECTS credits:	6
Semester:	1st (September-January)
Recommended components:	Linear algebra (1569), Groups and Rings (1585), Algebraic Equations (1596), Commutative Algebra (1600) While strictly speaking only some standard knowledge of groups and rings the student will benefit from a background in Galois Theory and Commutative Algebra.
Language of instruction:	Spanish or English depending on the students (students are allowed to ask questions and write homeworks and exams in either Spanish or English)

Course description

Every year the course is adapted to the interest of the group of students taking topics from several of the following topics: Elementary number theory (arithmetic functions, congruencies, quadratic reciprocity, Diophantine equations, continuous fractions, primality tests and factorization); Algebraic number theory (Number fields, algebraic integers, the class group, Minkowski Theorem, Dirichlet Unit Theorem, valuations); Elliptic curves (the group of an elliptic curve, torsion points, Frobenius endomorphism, factorization with elliptic curves); Criptography (algorithmic complexity, public key cryptosystems and associated number theory problems); analytic number theory (Dedekind zeta functions, number class formula, introduction to Class Field Theory)

Learning outcomes and competences

After completion of this course you will:

1. Know applications of algebraic and arithmetic techniques in the study the properties of the numbers and elliptic curves.

2. Know how to apply algebraic and arithmetic methods in cryptology.

3. Know how to calculate the complexity of an algorithm.

4. Know advanced cryptology primitives and how to implement them.

5. Know how to solve number theory problems.

Course contents

For the course 2016-2017

1. Number theory.

   Quadratic residuum. Algebraic integers and number fields. Quadratic and cyclotomic extensions.

2. Primality and factorization.

   The distribution of prime numbers. Primality tests and factorization algorithms

3. Algorithmic complexity.

   Polynomial time, deterministic and probabilistic algorithms in finite fields, number fields and elliptic curves. The P and NP classes of problems.

4. Public key cryptology.

   Cryptographic protocols using number fields, number fields and elliptic curves. Cryptanalisis, Proven security. Zero knowledge protocols. Secret sharing.

5. Elliptic curves.

   The group of an elliptic curve. Hasse Theorem. Algorithms with elliptic curves.

COMPUTER PRACTISES

1. Fields: Construction and manipulation with number fields using GAP.

2. Primality: Implementation of advance primality tests.

3. Factorization: Implementation of advance factorization algorithms.

4. Elliptic curves: Implementation of the arithmetic of elliptic curves and cryptographic protocols with them.

References

Main texts

1. Á. del Río, *Introducción a la criptografía matemática*, apuntes de la asignatura.

2. G.J. Janusz, *Algebraic number fields*, Academic Press 1973

Supplementary references

1. N. Koblitz, *A course in number theory and cryptography*, Springer 1988.

2. H. Cohen, *A course in computational algebraic number theory*, Springer 1993.

3. L. Washington, *Elliptic Curves.* Number Theory and Cryptography. Segunda edición, Chapman/Hall, 2008.

4. *GAP - Groups, Algorithms, Programming - a System for Computational Discrete Algebra.* http://www.gap-system.org/