Universitat Autònoma de Barcelona

2018/2019

Arithmetic

Code: 100113
ECTS Credits: 6

Degree	Type	Year	Semester
2500149 Mathematics	OT	4	0

Contact

Name: Marc Masdeu Sabate
Email: Marc.Masdeu@uab.cat

Use of languages

Principal working language: catalan (cat)
Some groups entirely in English: No
Some groups entirely in Catalan: Yes
Some groups entirely in Spanish: No

Teachers

Francesc Xavier Xarles Ribas
Marc Masdeu Sabate

Prerequisites

It is desirable to have completed all the compulsory algebra courses; concretely, students will be assumed to master the topics covered in Estructures Algebraiques.

Objectives and Contextualisation

The goal of this course is to introduce the student to arithmetic while, at the same time, offering a view of the methods that play a role in their analysis and resolution. Since there is a vast range of areas that fit inside number theory, this course will be based mainly on diophantine problems, from which algebraic number theory and arithmetic geometry will be introduced.

The course will be divided in three parts: (I) Primes; (II) Congruences and approximation; and (III) Elliptic curves. The common theme among these, which can serve as motivation - although this is not the focus of the course -, is the applications they have found in cryptography.

In the first part we will study the basic results on prime numbers and factorization, and we will see the first applications to cryptography.

The second part will be devoted to the law of quadratic reciprocity and to the study of one of the classical diophantine problems, namely the Pell equation.

In the third part we will introduce elliptic curves, emphasizing their applications to factorization and cryptography.

Contrary to what could be thought, number theory is one of the branches of mathematics that most closely resembles experimental sciences: its main object of study is something as concrete as numbers, which we know and use in our daily lives. This is why experimentation is a fundamental trait of number theory, and this is reflected in the course by using computer tools (mainly Sage) that allow us to discover, understand and solve many arithmetic phenomena.

Content

I. Primes

- Factorization
- The distribution of primes
- The integers modulo n
- Primality tests
- Diffie-Hellman and RSA

II. Congruences and approximation

- Quadratic reciprocity
- Continued fractions
- Sums of squares
- The Pell equation

III. Elliptic curves

- Definitions and basic properties
- Factorization of integers via elliptic curves
- Elliptic curve cryptography
- The Birch and Swinnerton-Dyer conjecture