Universitat Autònoma de Barcelona

2021/2022

Arithmetic

Code: 100113
ECTS Credits: 6

Degree	Type	Year	Semester
2500149 Mathematics	OT	4	0

The proposed teaching and assessment methodology that appear in the guide may be subject to changes as a result of the restrictions to face-to-face class attendance imposed by the health authorities.

Contact

Name: Marc Masdeu
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

Other comments on languages

Part of the bibliography may be in Catalan

Teachers

Francesc Xavier Xarles Ribas

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 four parts: (I) Divisibility and congruences; (II) Elliptic curves; (III) Quadratic reciprocity law; and (IV) Primality and factorization. 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 elliptic curves, emphasizing their applications to factorization and cryptography.

In the third part we will introduce the law of quadratic reciprocity and its consequences.

In the fourth part we will investigate algorithms to determine the primality of integers, or to find nontrivial factors of composites.

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.

Competences

- Actively demonstrate high concern for quality when defending or presenting the conclusions of ones work.
- Assimilate the definition of new mathematical objects, relate them with other contents and deduce their properties.
- Demonstrate a high capacity for abstraction.
- Develop critical thinking and reasoning and know how to communicate it effectively, both in ones own languages and in a third language.
- Effectively use bibliographies and electronic resources to obtain information.
- Students must be capable of applying their knowledge to their work or vocation in a professional way and they should have building arguments and problem resolution skills within their area of study.
- Students must be capable of collecting and interpreting relevant data (usually within their area of study) in order to make statements that reflect social, scientific or ethical relevant issues.
- Students must be capable of communicating information, ideas, problems and solutions to both specialised and non-specialised audiences.
- Students must develop the necessary learning skills to undertake further training with a high degree of autonomy.

Learning Outcomes

1. Actively demonstrate high concern for quality when defending or presenting the conclusions of ones work.
2. Develop critical thinking and reasoning and know how to communicate it effectively, both in ones own languages and in a third language.
3. Effectively use bibliographies and electronic resources to obtain information.
4. Students must be capable of applying their knowledge to their work or vocation in a professional way and they should have building arguments and problem resolution skills within their area of study.
5. Students must be capable of collecting and interpreting relevant data (usually within their area of study) in order to make statements that reflect social, scientific or ethical relevant issues.
6. Students must be capable of communicating information, ideas, problems and solutions to both specialised and non-specialised audiences.
7. Students must develop the necessary learning skills to undertake further training with a high degree of autonomy.
8. Understand in-depth demonstrations of some theorems of advanced algebra and assimilate the definition of new algebraic structures and constructions, relating them with other knowledge and deducing their properties.
9. Use algebraic tools in different fields.

Content

I. Primes and congruences

- Divisibility
- Factorization of integers
- The integers modulo n
- Effective methods for inverses and exponentiation

- Diffie-Hellman and RSA

II. Elliptic curves

- Definition and group law
- Torsion points, rational points
- Curves over finite fields
- Elliptic curve cryptography
- Point counting

III. Quadratic reciprocity law

- Quadratic residues and Legendre symbol
- QRL and proof
- The Jacobi symbol
- Application: square roots modulo p

IV. Primality and factorization

- Primality
- Factorization algorithms
- Pollard's rho
- Factor bases
- Continued fractions
- Algorithms for the discrete logarithm

Methodology

This subject has two weekly hours of theory. Other than the supplied lecture notes, at some points of the course it will be useful to read additional bibliography or material provided by the teacher.

There will be sessions dedicated to solving problems. Each student will have to present one of the problems in the list resolved, in writing and delivered to the teacher. The doubts that may arise may be asked during the class or during the consultative hours of the teachers. Work on these problems is based on the concepts introduced in the theory class, the statements of the theorems, and their demonstrations, since very often the techniques will be similar.

During the seminars, we will use SAGE to solve a project.

In addition, the subject has a page in the "Virtual Campus" where the lists of problems, additional material and any information related to the subject will be uploaded.

Annotation: Within the schedule set by the centre or degree programme, 15 minutes of one class will be reserved for students to evaluate their lecturers and their courses or modules through questionnaires.

Activities

Title	Hours	ECTS	Learning Outcomes
Type: Directed			
Theory sessions	30	1.2	1, 2, 7, 5
Type: Supervised			
Practical sessions	6	0.24	2, 3
Problem Sessions	14	0.56	1, 2, 7, 3

Type: Autonomous			
Study theory	37	1.48	1, 5, 3
Work on problems and computer programming	60	2.4	1, 2, 7, 5, 3

Assessment

During the course the student will have to turn in a problem, worth 25% of the final grade. The student will have to code a Sage program to apply some of the techniques explained in class, among several proposals that will be made at the beginning of the course, and worth 20% of the final grade. There will also be an oral presentation worth 25%. The remainign part of the grade (30%) will be obtained from a final exam consisting of several problems.

The only second chances will be given for the final exam and/or the Sage project, as long as the grade in each part is above 3,5 / 10. It is important to underline that, in case of trying a second chance, the student gives up on the previous mark.

Assessment Activities

Title	Weighting	Hours	ECTS	Learning Outcomes
Final exam	30%	3	0.12	8, 1, 2
Oral exposition	25%	0	0	1, 2, 7, 6, 5, 3
Problems to turn in	25%	0	0	1, 2, 7, 4, 5, 3
Program	20%	0	0	1, 2, 7, 5, 3, 9

Bibliography

Main

W. Stein, *Elementary Number Theory: Primes, Congruences, and Secrets,* Springer-Verlag, Berlin, 2008.

J.-P. Serre, *A Course in Arithmetic,* GTM7, Springer, 1973.

N.Koblitz, *A Course in Number Theory and Cryptography,* GTM114, Springer, 1994.

Supplementary

I.N. Stewart, D.O. Tall, *Algebraic Number Theory*, Chapman and Hall, 1979.

Z.I. Borevich y I.R. Shafarevich, *Number Theory*, Academic Press, 1966.

L.J. Mordell, *Diophantine Equations,* Academic Press, 1969.

J. Neukirch, *Algebraic number theory,* Springer-Verlag 1999.

Software

Sagemath (sagemath.org) will be used throughout the course. In order to facilitat collaboration among peers, a private CoCalc server will be set up.