UAB
Universitat Autònoma de Barcelona

Arithmetic

Code: 100113
ECTS Credits: 6

2024/2025

Degree	Type	Year
2500149 Mathematics	OT	4

Contact

Name: Francesc Bars Cortina

Email: francesc.bars@uab.cat

Teaching groups languages

You can view this information at the end of this document.

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 and finite extension field Theory (basics on Galois Theory).

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) Infinity number of analysis over the rationals! (II) Elliptic Curves (III) Hasse principle. (IV) Arithmetic Geometry. 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.

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 one's 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 one's 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 one's work.
2. Develop critical thinking and reasoning and know how to communicate it effectively, both in one's 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

(Translate from Google traductor)

I. Conics and $ p $ -adic numbers Conics and quadratic residue law. P-adic numbers. Rational points Non-Archimedean analysis. Completion of bodies.II. Elliptical curves Definition and group law Torsion points, rational points Mordell's theorem. III. Algebraic Number Theory Domined by Dedekind. The class group of a body. Kummer attacking Fermat's last theorem. IV. A brushstroke in Arithmetic Geometry. * Non-singular flat curves * Non-Archimedean absolute points and values. * Dedekind domains and non-singularity.

Activities and Methodology

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 a work about some diophantine equation.	60	2.4	1, 2, 7, 5, 3

(From Google traductor)

This subject has two hours of theory per week. In addition to the course notes, at certain times it will be necessary to complete the content of the class explanations with consultations in bibliography or material provided by the teacher. There will be sessions dedicated to problem solving. Each student will have to present one of the problems of the list solved, in writing and delivered to the teacher. Questions that arise may be asked during class or during teacher consultation hours. The work on these problems is supported by the concepts introduced in theory class, the statements of the theorems, and their proofs. In the seminars a concrete application will be practiced to solve certain Diophantine equations. There will be a problem delivery by groups where it will be of some similar problem to the seminars. There will be a list of works, where the student can choose one, or propose it himself to do a small work on that topic. In addition, the subject has a page on the "virtual campus" where the lists of problems, additional material and any information related to the subject will be posted. Note: 15 minutes of a class will be reserved, within the calendar established by the center / degree, so that the students fill in the surveys of evaluation of the performance of the teaching staff and of evaluation of the subject / module.

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.

Assessment

Continous Assessment Activities

Title	Weighting	Hours	ECTS	Learning Outcomes
A collective problem to deal	25%	0	0	1, 2, 7, 5, 3, 9
An individual work on a diophantine equation with oral exposition in a video	30%	0	0	1, 2, 7, 6, 5, 3
Final exam	15%	3	0.12	8, 1, 2
Problems to turn in	30%	0	0	1, 2, 7, 4, 5, 3

(From google translator)

During the course, different exercises will be assigned from a list that each student can submit individually, which will count for 30% of the final grade. There will also be a specific joint problem where each student will have to present individually and will count 25% of the course grade. Each student will be assigned a work from a list (but which can be proposed to the other teacher, as long as the theory teacher accepts it) where he will have to make an oral presentation with a video of at most 10 minutes, this work will correspond to 30% of the grade of the course. The rest of the grade (15%) will be obtained from a final exam where a problem will have to be solved with a few sections. Only the final exam can be retaken. It is important to note that in the event of applying for a grade, the student waives the previous grade. A student can give up making the deliveries of

problems and / or work, communicating it before to the professor of theory and that % would go to the final examination of the Arithmetic undergraduated course.

Students with a single assessment of Arithmetic, and who have officially requested it, will only take the final exam of the subject directly, having to obtain a grade equal to or higher than 5 out of 10 in order to pass the subject. If they do not pass, they will have the recovery exam.

Bibliography

Main

K.Kato, N.Kurokawa, T.Saito, Number Theory 1, Fermat's Dram. Translation of Mathematical Monographs, vol. 186, 1996, AMS.

D. Lorenzini. An invitation to Arithmetic Geometry. Graduate Studies in Mathematics, vol 9, 1996, AMS.

Supplementary

A.R. Omondi. Criptography arithmetic: algorithms and harware architectures, Advances in Information Security (vol.77), 2020. https://link.springer.com/book/10.1007/978-3-030-34142-8

A. Granville, Number Theory Revealed: a Masterclass. AMS, 2019.

A. Lozano-Robledo: Elliptic Curves, modular forms and their L-functions. Student Mathematical Library, vol. 58. AMS (2011).

S. Lang: Cyclotomic Fields I and II. GTM121, Springer, 1990, ISBN: 0-387-96671-4

M.Papikian: Drinfeld modules. Graduate Texts in Mathematics, 296. *Springer, Cham,* 2023. xxi+526 pp. ISBN: 978-3-031-19706-2

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.

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

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

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

K.Kato, N.Kurokawa,T.Saito, Number Theory 2, introduction to Class Field Theory. Translations of Mathematical Monographs, vol.240, AMS (1998).

N.Kurokawa, M.Kurihara, T.Saito, Number Theory 3, Iwasawa Theory and modular forms. Translations of Mathematical Monographs, vol.242, AMS (2012).

J.J.Silverman, The arithmetic of Elliptic Curves, GTM 106, Springer.

J.J. Silverman, The arithmetic of Dynamical Systems, GTM 241, Springer.

J.J. Silverman, A friendly introduction to Number Theory, Pearson Modern Classics series.

M.Hindry, J.J.Silverman, Diophantine Geometry: an introduction. GTM 201, Springer.

J.Hoffstein, J.Pipher, J.J.Silverman, An introduction to mathematical cryptography, Springer Verlag.

Software

Magma online calculator or Sagemath (sagemath.org) may be used throughout the course.

Language list

Name	Group	Language	Semester	Turn
(PAUL) Classroom practices	1	Catalan	second semester	morning-mixed
(SEM) Seminars	1	Catalan	second semester	afternoon
(TE) Theory	1	Catalan	second semester	morning-mixed