34953 - NT - Number Theory

**Coordinating unit:** 200 - FME - School of Mathematics and Statistics  
**Teaching unit:** 749 - MAT - Department of Mathematics  
**Academic year:** 2018  
**Degree:** MASTER'S DEGREE IN ADVANCED MATHEMATICS AND MATHEMATICAL ENGINEERING (Syllabus 2010). (Teaching unit Optional)  
**ECTS credits:** 7,5  
**Teaching languages:** English

**Teaching staff**

**Coordinator:** ANA RIO DOVAL  
**Others:** Primer quadrimestre:  
JORDI GUARDIA RUBIES - A  
JOAN CARLES LARIO LOYO - A  
ANA RIO DOVAL - A

**Prior skills**

Basic knowledge of algebraic structures: groups, rings and fields.

**Requirements**

Basic material covered in any standard courses on arithmetic, group theory and Galois theory. Although it is not strictly necessary, any background on algebraic curves, elliptic curves and basic number theory. But the course will be completely self-contained.

**Degree competences to which the subject contributes**

**Specific:**
1. **RESEARCH.** Read and understand advanced mathematical papers. Use mathematical research techniques to produce and transmit new results.  
2. **CALCULUS.** Obtain (exact or approximate) solutions for these models with the available resources, including computational means.  
3. **CRITICAL ASSESSMENT.** Discuss the validity, scope and relevance of these solutions; present results and defend conclusions.  
4. **SELF-DIRECTED LEARNING.** Detecting gaps in one's knowledge and overcoming them through critical self-appraisal. Choosing the best path for broadening one's knowledge.  
5. **EFFICIENT ORAL AND WRITTEN COMMUNICATION.** Communicating verbally and in writing about learning outcomes, thought-building and decision-making. Taking part in debates about issues related to the own field of specialization.  
6. **THIRD LANGUAGE.** Learning a third language, preferably English, to a degree of oral and written fluency that fits in with the future needs of the graduates of each course.  
7. **TEAMWORK.** Being able to work as a team player, either as a member or as a leader. Contributing to projects pragmatically and responsibly, by reaching commitments in accordance to the resources that are available.  
8. **EFFECTIVE USE OF INFORMATION RESOURCES.** Managing the acquisition, structure, analysis and display of information from the own field of specialization. Taking a critical stance with regard to the results obtained.
34953 - NT - Number Theory

Teaching methodology

Most of the lectures will take place on the blackboard, explaining carefully the contents of the course and providing as much explicit examples, exercises and applications as possible. The students will be encouraged to consult suitable references and to discuss between them and with the professor in order to achieve a good understanding of the material.

Learning objectives of the subject

1) Algebraic number theory.
2) Arithmetic of elliptic and hyperelliptic curves
3) Applications

The material covered in this course interplays with topics of applied arithmetic and number theory (primality testing) and algebraic geometry (curves of low genus)

Study load

<table>
<thead>
<tr>
<th>Total learning time: 187h 30m</th>
<th>Hours large group:</th>
<th>60h</th>
<th>32.00%</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Self study:</td>
<td>127h 30m</td>
<td>68.00%</td>
</tr>
</tbody>
</table>

Content

**Algebraic Number Theory**

Learning time: 93h 45m

- Theory classes: 30h
- Self study: 63h 45m

**Elliptic Curves**

Learning time: 93h 45m

- Theory classes: 30h
- Self study: 63h 45m

Qualification system

There will be a final exam. Optionally the qualification might be obtained based on:

1) Active participation of the student during the course,
2) Resolution of exercises suggested in class and,
3) Elaboration of a document in which the student develops in more detail and depth some of the material of the course.

Regulations for carrying out activities

Solved exercises and works must be delivered on the last day of the course.
34953 - NT - Number Theory

Bibliography

Basic:


Others resources:

Computer material

SAGE

Mathematical Software

Matlab

Mathematical software