UNIVERSITÀ
DEGLI STUDI DI MILANO-BICOCCA

COURSE SYLLABUS

Number Theory and Criptography

2526-1-F4002Q032

Aims

In line with the educational objectives of the Degree in Mathematics, the course aims to provide the student with some of the fundamental concepts, methods and some techniques of Number theory, essential for understanding the main asymmetric Cryptographic systems based on modular arithmetic or on elliptic curves over finite fields.
The student is expected to have knowledge of main probabilistic primality tests, the deterministic test AKS; the knowledge of the structure of the group of elliptic curves over finite fields, with applications to the problem of discrete logarithm and of factorisation. It is also expected they have the ability to give proofs presented in the course, using given techniques to solve easy problems and the ability to study some more details of results presented during the course.

Learning objectives and expected outcomes, formulated according to the five Dublin Descriptors:

Knowledge and understanding:
Students will acquire advanced knowledge in Number Theory, with particular emphasis on modular arithmetic, elliptic curves over finite fields, probabilistic and deterministic primality tests, and the mathematical foundations of public-key cryptographic systems. This knowledge will build upon a solid undergraduate background and will provide insight into the algebraic and arithmetic structures underlying modern cryptographic protocols.

Applying knowledge and understanding:
Students will be able to apply the learned techniques to critically analyze cryptographic algorithms based on number-theoretic problems (e.g., factorization, discrete logarithm), and to solve both theoretical and computational problems related to the topics covered in the course.

Making judgements:
Students will develop the ability to assess the mathematical soundness and security of cryptographic protocols, to interpret theoretical results and proofs independently, and to identify relevant hypotheses and methods for generalization.

Communication skills:

Students will be able to present theoretical concepts and techniques clearly and rigorously, both in written and oral form, using appropriate mathematical language suited to both scientific and applied contexts.

Learning skills:
Students will be capable of independently exploring related or more advanced topics, consulting the mathematical literature and understanding specialized texts and research articles in Number Theory and cryptographic mathematics, also in English.

Contents

Some classical results in Number Theory are presented, with particular regard to factorizzation methods and primality tests, using modular arithmetic and Elliptic Curves.

Detailed program

- Integers and finite fields; Euler function; modular arithmetic
- Definition of a Cypher: public and private key
- Some topics about Prime numbers: Notes on Dirichlet's Theorem; Number Prime Theorem.
- An introduction to Dirichlet's characters.
- Prime numbers and factorization: pseudoprimes; primality tests (Fermat, Jacobj, Miller-Rabin AKS); (p-1)-pollard method for factorization; complexity of the alghoritms.
- Some remark about Riemann's zeta function; Euler'sFactorization; Riemann's hypothesis; extended Riemann's hypothesis and some consequence on primality tests.
- Diffie-Hellman cypher; discrete logarithm
- Elliptic curves; group of the points of an elliptic curve on a finite field.
- Endomorphisms.
- Torsion points and Weil pairing.
- Hasse Theorem
- Cryptosystems on elliptic curves.
- Discrete Logarithm on Elliptic Curves
- Digital Signature: DSA, ECDSA
- Isogenies and chryptographic attacks.

Prerequisites

Basic Algebra: algebraic structure; abelian groups; finite fields.

Teaching form

Lectures (8 credits). They will be of two different kind: they will give knowledge of basic definitions, relevant results and theorems. On the other side, we intend to give skills to use results and knowledge in solving exercises and analysing problems

Some exercise will be made available regularly on the e-learning website to encourage participation.

A hybrid teaching approach is used, that combines lecture-based teaching (DE) and interactive teaching (DI). DE involves detailed presentation and explanation of theoretical content. DI includes active student participation through exercises and problems, short presentations, group discussions, and group or individual work. It is not possible to precisely determine in advance the number of hours dedicated to DE and DI, as these methods are dynamically intertwined to adapt to the course's needs and promote a participatory and integrated learning environment, combining theory and practice.

Lectures (56 hours) and practical sessions/tutorials are conducted in person and are primarily in Italian, and when necessary, in English.

Textbook and teaching resource

Main reference books:

- N. Koblitz, A course in Number Theory and Cryptography, volume 114 of Graduate texts in Mathematics, Springer-Verlag, second edition, 1994..
- H.E. Rose, A course in Number Theory, II edizione, Oxford: Clarendon press, 1994
- Lawrence C. Washington, Elliptic Curves, Number Theory and Criptogtaphy CRCPress

Other help books:

- Maria Welleda Baldoni, Ciro Ciliberto, Giulia Maria Piacentini Cattaneo, Elementary Number Theory, Cryptography and Codes, 2009 Springer-Verlag Berlin Heidelberg
- Graham Everest, Thomas Ward Introduction to Number Theory, Springer-Verlag London Limited 2005
- A. Languasco, A. Zaccagnini, Introduzione alla Crittografia, Hoepli Editore, 2004

Semester

II term.

Assessment method

Written and Oral examination.

- The written part consists of exercises where the students show their ability in using methods and tools introduced in the course.
- The oral part consists of two parts:
  1) discussion about written part;
  2) the student may decide between:

1. to give a classical oral exam, where he must show his competence about subjects considered in the lectures, also giving motivations for applications of theoretical topics;
2. to give a talk about a particular subject, which was considered not very deeply in the course.

In any case, the oral exam must verify the full knowledge of the subjects considered in the course, and the capacity of the student to be rigorous in the exposition.

The final result is achieved considering the average between the mark obtained in written+discussion (together), and the mark obtained in the subsequent oral part.

Mark range: 18-30/30.

Office hours

By direct agreement.

Sustainable Development Goals

QUALITY EDUCATION