# Complementary mathematics II

Prof. Marco Antonio Pellegrini

***COURSE AIMS AND INTENDED LEARNING OUTCOMES***

The aim of this course is to provide the basic notions of Number Theory, considering both classical problems and applications to Cryptography, keeping an historical and didactical approach.

At the end of the course, the student will master fundamental notions of Algebra and learned the first concepts of Number Theory and Cryptography.

***COURSE CONTENT***

- Integer: the course begins with a brief review of the basic concepts concerning Integers and Classes of remainders modulo *n*. In particular, we will talk about divisibility and the Euclidean Algorithm, Diophantine equations and unique factorization. We will also see results on Mersenne primes, Fermat primes and perfect numbers, the divisibility criterions, the solution of linear congruences and the Euler function.

- Some cryptographic applications: affine ciphers, block cipher, Vigenère’s cipher and stream ciphers.

Public key cryptography: we will also describe the RSA method and the problem of digital signature.

- Gaussian integers: we will study the ring of the Gaussian integers, with the aim of determine which integers can be written as the sum of two squares. We will also use the Gaussian integers to construct Pythagorean triples.

- Fermat’s last theorem: we will prove this theorem in the case of 4th powers, following Fermat proof, based on the infinite descent method.

***READING LIST***

The main reference is the handouts provided by the teacher on the platform Blackboard. For a deeper understanding of the topics, we recommend:

J. Kraft, L. Washington, *An introduction to Number Theory with Cryptography, Second Edition,* Chapman and Hall/CRC, 2018.

M. Cozzens, S.J. Miller, *The Mathematics of Encryption, AMS*, 2013.

***TEACHING METHOD***

The course consists of lessons on the blackboard. Students can find numerous exercises in the books listed in the Reading List.

***ASSESSMENT METHOD AND CRITERIA***

The exam consists of an oral test, which has a duration of 30-35 minutes and in which the theoretical preparation is tested and the student's exhibition capacity. During this oral exam, the student will be asked to describe some concepts seen throughout the course, ado to prove some results.

The final evaluation will assess the candidates’ explanatory efficacy, clearness and accuracy.

***NOTES AND PREREQUISITES***

It is assumed that the student already has basic notions of Algebra. Usually these notions are acquired during the first year of the Mathematics degree course.

*Further information can be found on the lecturer's webpage at http://docenti.unicatt.it/web/searchByName.do?language=ENG or on the Faculty notice board.*