lmat2440

2022

Number theory

5.00 credits	30.0 h + 15.0 h	Q1

Teacher(s)	Caprace Pierre-Emmanuel ;Pereira Olivier ;
Language :	French > English-friendly
Place of the course	Louvain-la-Neuve
Learning outcomes	
Evaluation methods	The assessment is based on a written exam, testing the knowledge and understanding of the theoretical notions, the examples and fundamental results, the ability to develop a consistent reasoning, and the mastery of the proof techniques introduced during the lectures. One or several mini-projects may be proposed during the quadrimester, and contribute to a maximum of 25% of the final grade for the course. This contribution is taken into account only if it is beneficial to the student.
Teaching methods	The course is taught by means of theoretical lectures and exercise sessions. During the sessions, the students are invited to make suggestions and formulate their ideas to advance the course on the basis of their preliminary knowledge.
Content	This activity consists in illustrating various aspects of number theory, including some that can be applied to cryptography. The following themes will be tackled. - Modular arithmetic: Chinese remainder theorem, quadratic reciprocity. - Rational quadratic forms: p-adic numbers and local-global principle. - Analytic methods: zeta function and Dirichlet's theorem. - Projective cubics: arithmetic properties of elliptic curves. - Algorithmic number theory: primality tests, factorization. - Construction of objects relevant to cryptography: elliptic curves and cryptosystems. The balance between those parts and the details of the program may vary from year to year.
Inline resources	Moodle website https://moodle.uclouvain.be/
Bibliography	R. Crandall, C.B. Pomerance : Prime Numbers: A Computational Perspective, Springer, 2005. H. Davenport : The higher arithmetic. An introduction to the theory of numbers. 8th edition, Cambridge UP, 2008. K. Ireland, M. Rosen : A classical introduction to modern number theory, Springer, 2d edition, 1991. N. Koblitz: A Course in Number Theory and Cryptography, Springer, 2nd edition, 1994. J.P. Serre: Cours d'arithmétique, PUF, 1970.
Faculty or entity in charge	MATH

Programmes containing this learning unit (UE)

Program title	Acronym	Credits	Prerequisite	Learning outcomes
Additionnal module in Mathematics	APPMATH	5		🔍
Master [120] in Mathematics	MATH2M	5		🔍
Master [120] in Electrical Engineering	ELEC2M	5		🔍
Master [120] in Computer Science and Engineering	INFO2M	5		🔍
Master [120] in Mathematical Engineering	MAP2M	5		🔍
Master [120] in Data Science Engineering	DATE2M	5		🔍
Master [120] in Data Science: Information Technology	DATI2M	5		🔍