UCLouvain

lmat2440

2022

Théorie des nombres

5.00 crédits	30.0 h + 15.0 h	Q1

Enseignants	Caprace Pierre-Emmanuel ;Pereira Olivier ;
Langue d'enseignement	Français > English-friendly
Lieu du cours	Louvain-la-Neuve
Préalables	Il est recommandé que l'étudiant·e maitrise les notions fondamentales de l'algèbre linéaire telles que développées par exemple dans les cours LMAT1131 ou LEPL1101.
Thèmes abordés	Initiation à divers aspects de la théorie des nombres et de ses méthodes, en particulier en vue de ses applications à la cryptographie mathématique.
Acquis d'apprentissage	**A la fin de cette unité d'enseignement, l'étudiant est capable de :** Contribution du cours aux acquis d'apprentissage du programme de master en mathématique. A la fin de cette activité, l'étudiant aura progressé dans sa capacité à: - Connaître et comprendre un socle fondamental des mathématiques. Il aura notamment développé sa capacité à: -- Choisir et utiliser les méthodes et les outils fondamentaux de calcul. -- Reconnaître les concepts fondamentaux d'importantes théories mathématiques actuelles. -- Etablir les liens principaux entre ces théories. - Faire preuve d'abstraction, de raisonnement et d'esprit critique. Il aura notamment développé sa capacité à: -- Dégager les aspects unificateurs de situations et expériences différentes. -- Raisonner dans le cadre de la méthode axiomatique. 1 -- Construire et rédiger une démonstration de façon autonome, claire et rigoureuse. - Analyser un problème mathématique et proposer des outils adéquats pour l'étudier de façon autonome. Acquis d'apprentissage spécifiques au cours. A la fin de cette activité, l'étudiant sera capable de: - résoudre des équations dans des anneaux d'entiers modulaires; - déterminer des conditions d'existence de solutions de certaines équations diophantiennes; - appliquer des résultats d'analyse mathématique à l'étude des nombres premiers; - appliquer des résultats d'arithmétique modulaire à la construction d'algorithmes utilisés en cryptographie. Mode d'évaluation des acquis des étudiants L'évaluation se fait sur base d'un examen écrit. On y teste la connaissance et la compréhension des notions, des exemples et des résultats fondamentaux, la capacité de construire un raisonnement cohérent, la maîtrise des techniques de démonstration introduites pendant le cours.
Modes d'évaluation des acquis des étudiants	L'évaluation se fait sur base d'un examen écrit. On y teste la connaissance et la compréhension des notions, des exemples et des résultats fondamentaux, la capacité de construire un raisonnement cohérent, la maîtrise des techniques de démonstration introduites pendant le cours. Un ou plusieurs mini-projets pourront être proposés durant le quadrimestre et intervenir pour maximum 25% dans la note finale pour ce cours. Cette contribution n'interviendra que si elle est favorable à la note finale de l'étudiant.e.
Méthodes d'enseignement	Le cours est donné sous forme de cours magistraux et de séances de travaux pratiques. Pendant les séances, les étudiants sont appelés à faire des suggestions et formuler des idées pour faire avancer le cours en se basant sur leurs connaissances préalables.
Contenu	Cette activité consiste à illustrer divers aspects de la théorie des nombres, y compris certains qui sont applicables à la cryptographie. Les contenus suivants sont abordés dans le cadre du cours. - Arithmétique modulaire : théorème chinois des restes et loi de réciprocité quadratique. - Formes quadratiques rationnelles : corps de nombres p-adiques et principe local-global. - Méthodes analytiques : fonction zêta et théorème de Dirichlet. - Cubiques projectives : propriétés arithmétiques des courbes elliptiques. - Théorie algorithmique des nombres: tests de primalité, factorisation. - Construction d'objets utiles en cryptographie: courbes elliptiques, systèmes de chiffrement.

	L'équilibre entre les différentes parties et les détails du programme ci-dessus sont susceptibles de varier d'année en année.
Ressources en ligne	Site Moodle https://moodle.uclouvain.be/
Bibliographie	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.
Faculté ou entité en charge:	MATH

Programmes / formations proposant cette unité d'enseignement (UE)

Intitulé du programme	Sigle	Crédits	Prérequis	Acquis d'apprentissage
Approfondissement en sciences mathématiques	APPMATH	5		
Master [120] en sciences mathématiques	MATH2M	5		
Master [120] : ingénieur civil électricien	ELEC2M	5		
Master [120] : ingénieur civil en informatique	INFO2M	5		
Master [120] : ingénieur civil en mathématiques appliquées	MAP2M	5		
Master [120] : ingénieur civil en science des données	DATE2M	5		
Master [120] en science des données, orientation technologies de l'information	DATI2M	5		