UCL Faculté des sciences

SC

MATH2380 Théorie des nombres

[30h] 3 crédits

Cette activité se déroule pendant le 1er semestre

Enseignant(s):	Jean-Jacques Quisquater, Jean-Jacques Quisquater (supplée Jean-Pierre Tignol), Jean-Pierre Tignol
Langue d'enseignement :	français
Niveau :	cours de 2ème cycle

Objectifs (en terme de compétences)

Le cours vise à donner les bases conceptuelles et les méthodes permettant 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;
- effectuer des calculs dans le groupe des points de certaines cubiques projectives sur les corps d'entiers modulaires.

Objet de l'activité (principaux thèmes à aborder)

Initiation à divers aspects de la théorie des nombres et de ses méthodes, en particulier en vue de ses applications à la cryptographie mathématique.

Résumé : Contenu et Méthodes

1. Arithmétique modulaire : théorème chinois des restes et loi de réciprocité quadratique;
2. Formes quadratiques rationnelles : corps de nombres p-adiques et principe local-global
3. Méthodes analytiques : fonction zêta et théorème de Dirichlet;
4. Cubiques projectives : propriétés arithmétiques des courbes elliptiques.

L'équilibre entre les différentes parties et les détails du programme ci-dessus sont susceptibles de varier d'année en année.
Méthodes: Exposés théoriques

Autres informations (Pré-requis, Evaluation, Support, ...)

Pré-requis : Eléments d'algèbre linéaire du niveau du premier cycle.
Mode d'évaluation : L'examen est oral. Il comporte la présentation d'un travail personnel développant un aspect de la théorie des nombres et des questions de synthèse sur l'ensemble du cours.
Support :
K. Ireland, M. Rosen : A classical introduction to modern number theory, Springer , 2d edition, 1991
J.P. Serre, Cours d'arithmétique , PUF, 1970
J.H. Silverman, The arithmetic of elliptic curves, Springer, 1986.

Autres crédits de l'activité dans les programmes

INFO21	Première année du programme conduisant au grade d'ingénieur civil informaticien	(3 crédits)
INFO22	Deuxième année du programme conduisant au grade d'ingénieur civil informaticien	(3 crédits)
MAP21	Première année du programme conduisant au grade d'ingénieur civil en mathématiques appliquées	(3 crédits)
MAP22	Deuxième année du programme conduisant au grade d'ingénieur civil en mathématiques appliquées	(3 crédits)
MAP23	Troisième année du programme conduisant au grade d'ingénieur civil en mathématiques appliquées	(3 crédits)
MATH22/E	Deuxième licence en sciences mathématiques (Economie mathématique)	(3 crédits)
MATH22/G	Deuxième licence en sciences mathématiques	(3 crédits)
MATH22/S	Deuxième licence en sciences mathématiques (Statistique)	(3 crédits)