Université Paul Sabatier 2018/2019

L3 ESR : Propositions de sujets de travail autonome

Primalité

Le principal protocole de cryptage actuel, RSA, repose sur la possibilité de produire de grands nombres premiers. Le but de ce projet serait de comprendre RSA, d'étudier quelques tests de primalité significatifs et leur "complexité" et de les appliquer à quelques grands nombres de Mersenne (nombres de la forme $2^p - 1$ où p est premier ; tous les records récents dont de ce type).
Références principales :
"Cours d'algèbre, primalité, divisibilité, codes" de Michel Demazure.
"Algorithmique et cryptographie" de Guy Robin.

Factorisation

Le principal protocole de cryptage actuel, RSA, repose sur la difficulté de factoriser de grands nombres entiers. Le but de ce projet serait de comprendre RSA, d'étudier quelques algorithmes de factorisation significatifs et leur "complexité" et de les appliquer à quelques grands nombres tirés de l'histoire des attaques contre RSA.
Références principales :
"The joy of factoring" de Samuel S. Wagstaff Jr.
"Algorithmique et cryptographie" de Guy Robin.

Transcendance

Les preuves successives de la transcendance de e (par Hermite) et de celle de π (par Lindemann) font partie des joyaux des mathématiques. Le but de ce projet serait d'aborder les méthodes de transcendance les plus accessibles et, si possible, leurs liens avec l'approximation diophantienne (approximation des irrationnels par les rationnels).
Références principales :
"Transcendental number theory" de Alan Baker.
"Transcendental numbers" de Carl Ludwig Siegel.

Arithmétique de l'infini

Il y a une infinité de nombres entiers, mais il y a "encore plus" de nombres réels ; et "encore plus" de fonctions de $\mathbf{R}$ dans $\mathbf{R}$ ... mais "pas plus" de fonctions *continues* ! L'arithmétique de l'infini, inventée de toutes pièces par Cantor, permet de préciser et d'enrichir ces énoncés, et même de raisonner par "récurrence" sur ces infinis. Le but de ce projet serait de comprendre l'arithmétique des cardinaux et des ordinaux infinis.
Références principales :
"Théorie axiomatique des ensembles" de Jean-Louis Krivine.
"Basic Set Theory" de A. Shen et N.K. Vereshchagin.