L3 MAPI : Propositions de sujets de travail autonome

Primalité et cryptage RSA

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 sont de ce type). On peut aussi s'intéresser aux méthodes de factorisation de grands nombres, qui sont des attaques possibles contre RSA.
Référence principale : "Mathématiques et technologie" de Christiane Rousseau et Yvan Saint-Aubin, chapitre 7. (Également : "Algorithmique et cryptographie" de Guy Robin.)

Générateurs aléatoires

Selon John Von Neumann, l'un des inventeurs de l'Ordinateur, "Anyone who considers arithmetical methods of producing random digits is, of course, in a state of sin" [1]. Pourtant tous les systèmes informatiques actuels proposent des générateurs de nombres aléatoires, et ces derniers sont très fréquemment utilisés (par exemple pour organiser des simulations, des tests ...). Le but de ce projet serait de comprendre les méthodes de générations de nombres pseudo-aléatoires et la façon dont on teste leur "randomness".
Référence principale : "Mathématiques et technologie" de Christiane Rousseau et Yvan Saint-Aubin, chapitre 8. (Également : "The Art of Computer Programming" de Donald E. Knuth, chapitre 3.)

L'algorithme PageRank de Google

Pour ordonner les liens qui répondent à une requête selon l'intérêt probable pour l'utilisateur, Google utilise l'algorithme PageRank qui repose sur de l'algèbre linéaire (puissances de matrices) et les probabilités discrètes (chaînes de Markov). Le but de ce projet serait de comprendre et d'implémenter Pagerank, ou une version simplifiée.
Référence principale : "Mathématiques et technologie" de Christiane Rousseau et Yvan Saint-Aubin, chapitre 9.

Compression d'image : le standard JPEG

Le standard de compression d'image JPEG (fichiers jpg) est un compromis entre l'efficacité et la non-perte d'information. Il repose sur de l'algèbre linéaire (matrices, bases orthogonales) et un peu de trigonométrie élémentaire. Le but de ce projet serait de comprendre et d'implémenter compression et décompression et de les tester sur des exemples bien choisis.
Référence principale : "Mathématiques et technologie" de Christiane Rousseau et Yvan Saint-Aubin, chapitre 12.

1. "Quiconque envisage des méthodes arithmétiques pour produire des nombres aléatoires est, bien entendu, en état de péché."