Sujets de Projets d'Initiation à la Recherche 2012-2013

Master 1 Mathématiques (Cryptis)

Les projets seront réalisés par groupes de 2 ou 3. Vous pouvez contacter les enseignants et prendre rendez-vous pour vous faire une idée. Nous ferons ensuite une réunion pour décider collégialement de la répartition des projets (au cas où plusieurs groupes voudraient le même). Pour contacter les enseignants : prenom.nom-at-unilim.fr

Olivier Ruatta ⋆ **Distance sous-espace et codes sous-espace**
Résumé : (théorie des codes, décodage) Dans ce projet on s'intéresse à une famille de codes dits sous-espaces. On considère un espace vectoriel E et un ensemble de sous-espaces de cet espace. On définit alors une distance entre ces sous-espaces tenant compte de la dimension des sous-espaces et de leur intersection. En représentant ces sous-espaces par des matrices, on obtient des codes correcteurs d'erreurs. Sauf qu'il ne corrige pas pour la distance de Hamming, mais pour la distance sous-espace. Ces métriques ont des propriétés très différentes. Il s'agit d'étudier ces codes d'être capable de faire un programme permettant de traiter des exemples non triviaux pour illustrer votre rapport (codage, décodage) et comprendre son utilisation en "Network Coding". Si le temps le permet, on évoquera des propriétés cryptographiques potentielles de ces codes.
Pré-requis : Théorie des codes, algèbre linéaire.
Références :
Koetter, R. and Kschischang, F.R. **Coding for Errors and Erasures in Random Network Coding** arxiv.org/pdf/cs.IT/0703061 ou
http ://ieeexplore.ieee.org/xpls/abs_all.jsp ?arnumber=4567581&tag=1.
Shu-Tao Xia and Fang-Wei Fu. **Johnson Type Bounds on Constant Dimension Codes**. http ://arxiv.org/abs/0709.1074.
Moshe Schwartz and Tuvi Etzion. **Codes and Anticodes in the Grassman Graph** . http ://dx.doi.org/10.1006/jcta.2001.3188.

Pierre Dusart et Thierry Berger ⋆ **Tests statistiques sur certains générateurs pseudo-aléatoires**

Les LFSR (Linear Feedback Shift Register) sont des automates linéaires utilisés dans de nombreuses applications, entre autres pour la génération de nombres aléatoire dans les méthodes de simulations et comme brique de base dans la construction d'algorithmes de chiffrement à clé secréte et la génération de suites pseudo-aléatoires cryptographiquement robustes.

L'objectif de ce travail est d'appliquer certains tests de la batterie U01 développée par des chercheurs canadiens à des LFSR par blocks appelés "block-ring LFSR" développés par des chercheurs de Limoges. Le travail demandé consistera à comprendre et se familiariser avec ces générateurs, comprendre les tests, les mettre en oeuvre et interpéter les résultats en particulier en les comparant avec les résultats obtenus pour d'autres générateurs.

François Laubie ⋆ **Initiation aux nombres p-adiques.**

Construction de Z_p par les développements de Hensel, par completion topologique, par limite projective. Groupes de galois des Z_p extensions.
Réference principale : Les nombres p-adique, Y. Amice, PUF

C. Clavier ⋆ **Détermination d'une borne inférieure d'un éventuel nombre parfait impair**

Résumé : Un nombre parfait est un entier égal à la somme de ses diviseurs (lui-même excepté). 6 et 28 sont deux exemples de nombres parfaits. Tous les nombres parfaits connus actuellement sont pairs, et la question non résolue depuis l'antiquité de l'existence d'un nombre parfait impair constitue la conjecture la plus ancienne des mathématiques. Faute de pouvoir prouver la non-existence de tels nombres, des résultats toujours plus évolués permettent d'établir des contraintes de plus en plus fortes sur de tels nombres : borne inférieur sur sa valeur, nombre total de facteurs premiers, nombre de facteurs premiers distincts,...

Après avoir établi un état de l'art sur la recherche des nombres parfaits impairs, vous analyserez un article décrivant une méthode permettant de générer – sous la forme d'un arbre de contradictions – une preuve qu'un nombre parfait impair ne peut pas être inférieur à 10^{300}. La partie principale de votre travail consistera à étudier et comprendre cette méthode, et à l'implémenter pour générer la-dite preuve.

Paola Boito ⋆ **Moyennes géométriques de matrices.**
Résumé : La moyenne géométriques de deux nombres positifs $a\#b = \sqrt{ab}$ se généralise de manière assez naturelle au cône des matrices semi-définies positives. La moyenne de matrices $A\#B$ et ses généralisations répondent à la question de calculer le barycentre (dans un sens opportunément défini) d'un ensemble de données, question qui se présente dans la résolution de problèmes de statistiques, physique, information quantique, imagerie médicale. Dans ce projet nous proposons

- d'étudier la définition de $A\#B$ et son lien avec la métrique riemannienne dans l'espace des matrices semi-définies positives,
- d'étudier les méthodes de calcul de $A\#B$ et envisager les généralisations possibles au cas de plusieurs matrices,
- de mener des expériences numériques dans le cadre des applications aux problémes d'élasticité.

Références : T. Ando, Chi-Kwong Li, Roy Mathias, **Geometric means** ; Linear Algebra Appl. 385 (2004), 305–334.

Marc Rybowicz ⋆ **Composition modulaire et factorisation**
Résumé : Kedlaya et Umans ont publié récemment une méthode pour la composition modulaire qui donne l'algorithme de factorisation de polynômes de $\mathbb{F}_q[x]$ ayant la meilleure complexité *binaire* asymptotique connue. L'objet du travail est de :

- comprendre l'ensemble des techniques introduites par Kedlaya et Umans, potentiellement utiles dans d'autres contextes,
- étudier les freins ‡ une mise en oeuvre effective de ces techniques,
- si le temps le permet, étudier l'impact de ces résultats sur d'autres problèmes (comme par exemple sur le calcul modulo des ensembles triangulaires.

Références : KEDLAYA, K. S., AND UMANS, C. *Fast Polynomial Factorization and Modular Composition.* SIAM J. Computing 40, 6 (2011), 1767–1802. POTEAUX, A., AND SCHOST, E. *Modular composition modulo triangular sets and applications.* Submitted to Computational Complexity (2010). POTEAUX, A., AND SCHOST, E.

J.A Weil ⋆ **Décodage de codes non-commutatifs**
De nouvelles familles de codes, basés sur des anneaux non-commutatifs, ont éclos ces dernières années. L'objet de ce travail est d'étudier des méthodes de décodages d'une de ces familles (les codes de Gabidulin) et éventuellement voir comment les étendre à d'autres familles. Références : WACHTER, SIDORENKO, BOSSERT *Fast decoding of Gabidulin codes*