Sujet de thèse de Mathieu Roux

"Les séries de Dirichlet et l'analyse en moyenne des algorithmes de réduction de réseaux"

co-dirigé par Driss Essouabri (LMNO) et Brigitte Vallée (GREYC)

Sujet de thèse. C'est un sujet à l'interface entre la théorie analytique des nombres, la théorie des systèmes dynamiques, les probabilités, et l'algorithmique.

Lors de l'analyse précise du célèbre algorithme d'Euclide, effectuée avec des méthodes dynamiques, il apparaît de manière naturelle des séries de Dirichlet, qui sont des généralisées des séries Zeta du système dynamique sous-jacent à l'algorithme d'Euclide. Pour analyser précisément l'algorithme d'Euclide, et obtenir la distribution limite des principaux paramètres de l'algorithme (par exemple, son coût en « bits »), il est crucial de décrire les propriétés de telles séries de Dirichlet et d'évaluer en particulier la largeur d'une bande sans pôle à la gauche de $s = 1$.
Dans des travaux antérieurs, l'existence d'une telle bande est obtenue par des méthodes de systèmes dynamiques, qui ne donnent qu'un résultat sur l'existence d'une telle bande, et ne permettent pas d'évaluer sa largeur. Il s'agit lors de la thèse

1) de reprendre cette étude en choisissant le point de vue de la théorie analytique des nombres et d'étudier directement ces séries de Dirichlet. Peut-on ainsi obtenir des résultats précis sur la largeur d'une telle bande ?

2) d'analyser l'algorithme, non plus sur les rationnels (dont le développement en fraction continue (DFC) est fini) mais sur les irrationnels quadratiques (dont le DFC est périodique). On obtient d'autres séries de Dirichlet, pour lesquelles il faut évaluer la largeur de la bande sans pôles.

3) d'étendre l'étude à des algorithmes qui généralisent l'algorithme d'Euclide à de plus grandes dimensions (réduction de réseaux euclidiens). L'étude en dimension 2, introduit des généralisées des séries d'Eisenstein (formes de Maass), qui apparaissent naturellement dans la configuration de sortie de l'algorithme de Gauss. Leur étude est essentielle dans l'analyse du célèbre algorithme LLL.