

# Séminaire de théorie des nombres

Le 2 mai 2011 à 14h (à Chevaleret)

## Comment trouver des nombres premiers de manière déterministe

Exposé de Harald Helfgott (ENS Paris)

**Résumé :** Soit  $N$  grand. Comment peut-on trouver un nombre premier entre  $N$  et  $2N$  ?

Comme les nombres premiers sont assez denses, et comme on peut vérifier la primalité d'un nombre rapidement, donner un algorithme probabiliste pour trouver un nombre premier rapidement est une tâche très facile. Mais comment obtenir un algorithme déterministe ?

Nous verrons qu'il y a un algorithme qui marche en temps  $O(N^{1/3+\epsilon})$  – si le nombre de nombres premiers entre  $N$  et  $2N$  est impair, mais pas si il est pair !

[Issu d'un projet Polymath [collaboration massive]. Les participants principaux étaient E. Croot, H. Helfgott et T. Tao]