

---

**DIMITRIS KOUKOULOPOULOS**, Université de Montréal

*Irréductibilité de polynômes aléatoires de grand degré*

Considérons un polynôme unitaire aléatoire  $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$ , où  $a_j$  est choisi uniformément au hasard parmi 0 et 1, et indépendamment des autres coefficients. Odlyzko et Poonen ont conjecturé en 1993 que  $f(x)$  est irréductible avec probabilité  $\sim 1/2$  quand  $n \rightarrow \infty$ . Breuillard et Varjú ont prouvé cette conjecture sous l'hypothèse de Riemann généralisée. Dans cet exposé, je présenterai un travail conjoint récent avec Bary-Soroker et Kozma qui montre sans conditions que  $f(x)$  est irréductible avec probabilité  $\geq 1/1000$ . De plus, si nous conditionnons sur l'évènement que  $f(x)$  est irréductible, nous prouvons également que le groupe de Galois de  $f(x)$  contient le groupe alternatif  $A_n$  avec une probabilité conditionnelle  $\sim 1$ . Les preuves utilisent un mélange amusant d'idées issues de méthodes de crible, de l'arithmétique des polynômes sur des corps finis, de l'analyse de Fourier  $p$ -adique, des nombres premiers à chiffres restreints, de la théorie de Galois et de la théorie des groupes.