

**Irreducibility of random polynomials of large degree**

Dimitris Koukoulopoulos

*Université de Montréal*

Let  $f(x) = a_0 + a_1x + \cdots + a_{n-1}x^{n-1} + x^n$  be a random monic polynomial, where  $a_j$  is chosen uniformly at random from  $\{0, 1\}$  and independently of the other coefficients. In 1993, Odlyzko and Poonen conjectured that  $f(x)$  is irreducible with probability  $\sim 1/2$  when  $n \rightarrow \infty$ . Breuillard and Varjú proved that this expectation is indeed true under the Generalized Riemann Hypothesis. In this talk, I will present joint work with Bary-Soroker and Kozma that proves that  $f(x)$  is irreducible with probability  $\geq 1/1000$  for all large enough  $n$ . In addition, if we condition on the event that  $f(x)$  is irreducible, then we prove that the Galois group of  $f(x)$  contains the alternating group  $A_n$  with conditional probability  $\sim 1$ . The proofs use a fun mixture of ideas from sieve methods, the arithmetic of polynomials over finite fields,  $p$ -adic Fourier analysis, primes with restricted digits, Galois theory and group theory.