RANDOM WALKS ON FINITE FIELDS AND RANDOM POLYNOMIALS.

EMMANUEL BREUILLARD

Abstract

I will report on joint work with Peter Varju, in which we study random polynomials of large degree. Conditionally on the Riemann hypothesis for Dedekind zeta functions we show that random polynomials with integer coefficients and degree tending to infinity are irreducible with large probability, answering a question of Odlyzko and Poonen. The proof uses a sieve argument that involves the study of a random walk on the affine line over a finite field, which is a mod p analogue of the classical Bernoulli convolutions, and had been studied by Chung-Diaconis-Graham and Konyagin. The proof also hints at a connection with the celebrated Lehmer problem on Mahler measures.