Atelier
« Nouvelles approches en théorie probabiliste et multiplicative des nombres »
08-12 décembre 2014

Workshop
"New approaches in probabilistic and multiplicative number theory"
December 08–12, 2014

Permutations and sumsets of a random Poisson—Zipf set

Robin Pemantle*

pemantle@math.upenn.edu

Let M be a random set of integers greater than 1, containing each integer n independently with probability $1/n$. Let $S(M)$ be the sumset of M, that is, the set of all sums of subsets of M. How many independent copies of S must one intersect in order to obtain a finite set?

This problem is the limiting form of a problem arising in computational Galois theory: How many permutations must one sample uniformly from the symmetric group S_n before there is at least an epsilon probability that these permutations generate S_n even when an adversary replaces each one with a conjugate (another permutation of the same cycle type)?

Dixon showed in 1992 that $C(\log n)^{1/2}$ sufficed, and conjectured that $O(1)$ was good enough, which was proved shortly thereafter by Luczak and Pyber. Their constant was 2^{100} has not been improved until now, though various guesses have been made as to the actual number: 13, 12, 5, 4. We show in fact that 4 permutations suffice (equivalently, four copies of S have finite intersection).

This is joint work with Yuval Peres and Igor Rivin.

*Department of Mathematics, University of Pennsylvania, David Rittenhouse Lab., 209 S. 33rd Street, Philadelphia, PA 19104-6395, USA.