Faster algorithms for the Shortest Vector Problem

Oded Regev, Courant Institute, NYU

We give a randomized ~2^n-time algorithm for solving the Shortest Vector Problem (SVP) on n-dimensional lattices, improving on the previous best running time of 4^n by Micciancio and Voulgaris (STOC 2010). Despite being the fastest, the algorithm is arguably also the simplest in this line of work.

The main ingredients used are the discrete Gaussian distribution, an identity due to Riemann, and a way to transform samples from a distribution p into samples from the "square of p". Time permitting, we will also discuss an algorithm running in time 2^{n/2} that solves another hard lattice problem.

Joint work with Divesh Aggarwal, Daniel Dadush, and Noah Stephens-Davidowitz.