Computational complexity of lattice problems and cyclic lattices

Lenny Fukshansky, Claremont McKenna College

The classical theory of lattices in Euclidean spaces presents a wealth of hard problems from the stand-point of computational complexity. Two of the most famous such problems are SVP (the shortest vector problem) and SIVP (the shortest independent vector problem), both of which are known to be NP-hard. The hardness of these problems is crucial for the state of the art cryptographic algorithms. In fact, it is known that SIVP can always be reduced to SVP by a polynomial-time algorithm. On the other hand, it is rare that these two problems are actually equivalent. In this talk I will discuss some background of lattice problems and computational complexity, and then concentrate on a special very useful class of cyclic lattices, on which SVP and SIVP turn out to be equivalent with positive probability.