Lattices with Symmetry

Alice Silverberg, University of California, Irvine

For large ranks, there is no good algorithm that decides whether a given lattice has an orthonormal basis. But when the lattice is given with enough symmetry, in joint work with Hendrik W. Lenstra we construct a provably deterministic polynomial-time algorithm to accomplish this, based on the work of Craig Gentry and Mike Szydlo. The techniques involve algorithmic algebraic number theory, analytic number theory, commutative algebra, and lattice basis reduction.