Testing isomorphism of lattices over CM-orders.
Alice Silverberg, University of California, Irvine

A CM-order is an order equipped with an involution that mimics complex conjugation. We give a deterministic polynomial-time algorithm that decides whether two lattices over a given CM-order are isomorphic, and if so, finds such an isomorphism. This may be viewed as a special case of a principal ideal testing problem. An important ingredient is a technique introduced by Gentry and Szydlo in a cryptographic context. Our application of it hinges on a novel existence theorem for auxiliary ideals, which we deduce from a result of Konyagin and Pomerance in elementary number theory. This is joint work with Hendrik Lenstra.