1095-06-220

Lenny Fukshansky (lenny@cmc.edu), 850 Columbia Avenue, Claremont, CA 91711, and **Xun Sun*** (foxfur_32@hotmai.com), 168 E La Sierra Dr, Arcadia, CA 91006. *Complexity of lattice problems on cyclic lattices.*

Cyclic lattices are sublattices of $\mathbb{Z}^N$ that are preserved under the rotational shift operator. Cyclic lattices were introduced by D. Micciancio in 2002 and their properties were studied in the recent years by several authors due to their importance in cryptography. In particular, Peikert and Rosen showed that on cyclic lattices of prime dimension N, the shortest independent vectors problem SIVP reduces to the shortest vector problem SVP with a particularly small loss in approximation factor, as compared to general lattices. In this talk, we further investigate geometric properties of cyclic lattices, in particular proving that SVP is in fact equivalent to SIVP on a positive proportion of cyclic lattices in every dimension N. (Received September 09, 2013)