# Lattices with Symmetry

[Invited Talk]

Hendrik Lenstra

Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden, The Netherlands

hwl@math.leidenuniv.nl

## ABSTRACT

It is a notoriously difficult algorithmic problem to decide whether a given lattice admits an orthonormal basis. However, this problem becomes doable if the lattice is given along with a suitably large abelian group of symmetries. The lecture is devoted to a precise formulation of this result and to an outline of the algorithm that underlies its proof. One of the ingredients is an elegant algorithmic technique that C. Gentry and M. Szydlo introduced several years ago in the context of cryptography, but that can be recast in algebraic language. Other ingredients are taken from analytic number theory and from commutative algebra. Part of the work reported on was done jointly with Alice Silverberg and René Schoof.

## Categories and Subject Descriptors

I.1.2 [**Computing Methodologies**]: Symbolic and Algebraic Manipulation—*Algorithms*

## Keyword

lattices


*ISSAC'13,* June 26–29, 2013, Boston, Massachusetts, USA.
ACM 978-1-4503-2059-7/13/06 .