UNIVERSITÄT DES SAARLANDES
Fachrichtung 6.1 Mathematik
Prof. Dr. R. Schulze-Pillot

Universität des Saarlandes, E2 4, Zi. 321 - email: schulzep@math.uni-sb.de

UNIVERSITÄT DES SAARLANDES

Lecture on euclidean lattices and algorithms, summer semester 2017, Mi 10-12, SR 9

A lattice in euclidean space $\mathbb{R}^n$ is the set of linear combinations with integral coefficients of some fixed set of basis vectors of the space, which then also form a basis over the ring of integers $\mathbb{Z}$ of the lattice (which, of course, has infinitely many other bases).
The standard scalar product on $\mathbb{R}^n$ induces a positive definite symmetric bilinear form on the lattice. Classical reduction theory of quadratic forms is concerned with the study of bases of such a lattice which are minimal in some suitable sense, eg. length of basis vectors. The results are almost all effective, but algorithms based on them are exponential in the input length.
Algorithmic theory then deals with suitable weakenings of the classical concepts which allow faster computation, for example the concept of LLL-reduction. More generally, one studies vectors whose length is bounded by a fixed multiple of the length of a shortest vector in the lattice instead of insisting on finding such a shortest vector.
In this course I will first introduce the classical theory and then study recent results on the short vector problem and the closest lattice point problem from the algorithmic theory. Such results have applications e. g. in cryptography.

The course will be given in English if there are participants who don't understand lectures given in German, in German otherwise.

Prerequisites: Linear Algebra as learned in Linear Algebra I or Mathematik für Informatiker

Literature:

- Cohen: A course in computational algebraic number theory, Springer Verlag
- Micciancio, Goldwasser: Complexity of lattice problems - a cryptographic perspective