

Recent Trends in Algorithmic Geometry of Numbers

Friedrich Eisenbrand*

Abstract

The algorithmic geometry of numbers is a classical field of mathematics that was pioneered by Lagrange and Gauss with their work on binary quadratic forms more than 200 years ago. Questions concerning the representability of integers by quadratic forms and geometric techniques to answer them have fascinated mathematicians since then.

At least since the development of the LLL-algorithm more than 25 years ago, the algorithmic geometry of numbers has played an important role in the fields of computational complexity, cryptography, and optimization. Here, in particular, fundamental lattice problems like closest and shortest vectors of a lattice play a prominent role.

In this tutorial I will survey some results from the algorithmic geometry of numbers and its relation to algorithmic research. I plan to start with exemplary results from the origins of the field and build a bridge to recent algorithmic breakthroughs and intriguing open problems.

*EPFL, Station 8, 1015 Lausanne,
friedrich.eisenbrand@epfl.ch