

MATHEMATISCHES FORSCHUNGSINSTITUT OBERWOLFACH

Report No. 1/2005

Gitter und Anwendungen

Organised by
Christiane Bachoc (Bordeaux)
Eva Bayer-Fluckiger (Lausanne)
Gabriele Nebe (Aachen)

January 2nd – January 8th, 2005

ABSTRACT. The meeting focussed on lattices and their applications in mathematics and information technology. The research interests of the participants varied from engineering sciences, algebraic and analytic number theory, coding theory, algebraic geometry to name only a few.

Mathematics Subject Classification (2000): 11xx.

Introduction by the Organisers

Respecting the different backgrounds of the participants, most of the talks were aimed to a broad audience, among those nine survey talks invited by the organizers. This concept was very successful and opened many discussions and interdisciplinary interactions. It was also very fruitful for the many young participants. Also most of the non speakers took the opportunity to present their recent work via posters.

The theory of lattices has many applications and interactions with various other mathematical and technical disciplines such as information technology, topology, algebraic geometry, representation theory, combinatorics, number theory and modular forms to name only the most prominent ones. One of the most classical problems is the construction of dense lattice sphere packings. The densest lattice sphere packings are only known in dimensions up to 8 and, due to a recent work by H. Cohn and A. Kumar, also in dimension 24. A. Kumar gave a very illuminating talk on the strategy of their proof of this great result which uses certain linear programming techniques based on the fact that the minimal vectors of the Leech lattice form a very good design. Design techniques have also been used by B. Venkov to define the notion of strongly perfect lattices, which realize certain

local maxima of the density function and which are now classified up to dimension 12.

The theory of modular forms is one well established tool in the investigation of lattices as shown in the nice introduction by Krieg. Bannai applies this theory to bound the strength of designs provided by layers of unimodular lattices. On the other hand, lattices provide one important tool for the construction of modular forms. The last talk by Böcherer showed that in many situations all modular forms are linear combinations of theta-series.

Of increasing interest but computationally very difficult is the investigation of thin lattice sphere coverings. Vallentin and Schürmann developed new algorithms to find local optimal coverings and discovered lattice coverings better than the ones previously known.

Nguyen presented new reduction algorithms for lattices in small dimensions motivated by practical applications to cryptosystems. For certain applications in information technology not only the density of the lattice but also other properties that minimize the fading error play a role. It turns out that lattices constructed from algebraic number fields yield good codes for Rayleigh fading channels. These ideal lattices are also used to investigate the ring of integers in algebraic number fields as shown in the talk by Schoof and also in the applications of ideal lattices introduced by Bayer-Fluckiger. Strongly related to this is the application to Arakelov theory as illustrated in the talks by Bost and Künnemann.

Also Voronoi's classical theory of perfect forms (see Martinet's talk for an introduction) has new fruitful applications in number theory more precisely in the calculation of the homology of $GL_n(\mathbf{Z})$ as presented by Elbaz-Vincent.

Last but not least one should mention the talk by J.-P. Serre on BL-bases and unitary groups in characteristic 2.