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

Universität des Saarlandes, E2 4, Zi. 318 - email: schulzep@math.uni-sb.de

Im Sommersemester 2011 halte ich eine **Vorlesung** mit dem Thema

Ganzzahlige quadratische Formen und euklidische Gitter
(Integral quadratic forms and euclidean lattices).

The course can be given in english if participants wish so. An announcement in english is at: `www.math.uni-sb.de/ag/schulze/qf_2011_english.pdf`. Die Vorlesung beschäftigt sich mit einem Teilgebiet der Zahlentheorie, das enge Verbindungen zur Codierungstheorie und zu geometrischen Problemen (insbesondere Kugelpackungsproblemen) hat, die auch in der Optimierung eine Rolle spielen. Es findet auch Anwendungen in der Kryptographie. Die Vorlesung wendet sich an Studierende der Mathematik oder der Informatik, sie kann zum Einstieg in die Spezialisierung mit Ziel Bachelor/Master oder Staatsexamensarbeit benutzt werden.
Ganzzahlige quadratische Formen erhält man unter anderem, indem man ein $\mathbb{Z}$-Gitter L im euklidischen Raum $\mathbb{R}^n$ mit der durch das Standardskalarprodukt gegebenen symmetrischen Bilinearform betrachtet und dann einen Gittervektor durch seine (ganzzahligen) Koordinaten $x_1, \ldots, x_n$ bezüglich einer $\mathbb{Z}$-Basis des Gitters L beschreibt; im einfachsten Fall $L = \mathbb{Z}^n$ liefert das (bezüglich der Standardbasis) die quadratische Form $Q(x_1, \ldots, x_n) = \sum_{j=1}^{n} x_j^2$, allgemein erhält man

$$Q(x_1, \ldots, x_n) = \sum_{i,j=1}^{n} a_{ij} x_i x_j$$

mit einer symmetrischen Matrix $A = (a_{ij})$. Man sucht dann z. B. nach der Anzahl der ganzzahligen Lösungen einer solchen quadratischen Gleichung $Q(x_1, \ldots, x_n) = t$ sowie nach (bzgl. Q) kurzen Vektoren bzw. nach Gitterbasen aus kurzen Vektoren, das führt auf die Reduktionstheorie und auf Algorithmen wie den berühmten LLL-Algorithmus.
Vorkenntnisse: Anfängervorlesungen, Grundkenntnisse der elementaren Zahlentheorie, etwa aus der „Einführung in Algebra und Zahlentheorie (EAZ)“.

Die Vorlesung wird durch mein Seminar über binäre quadratische Formen und quadratische Zahlkörper (4-8 LP) ergänzt (ist aber von diesem unabhängig), bei Interesse können auch Übungen (weitere 3 LP) angeboten werden.
Sie ist bisher als 2-stündige Vorlesung mit 3 Leistungspunkten (Mo 10-12 Hs. 4) angekündigt, eventuell (insbesondere auf Wunsch potentieller TeilnehmerInnen) wird sie zur 4-stündigen Vorlesung (6 LP) heraufgestuft.

Literatur: (Weitere Literatur in der Vorlesung)

- J. Conway, N.J.A. Sloane: Sphere Packings, Lattices and Groups
- J. Martinet: Perfect Lattices in Euclidean Spaces
- J. W. S. Cassels: Rational Quadratic Forms