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 Wintersemester 2014/15 halte ich eine 2-stündige **Vorlesung** mit 2- stündigen Übungen (6CP) mit dem Thema

Algorithmische Zahlentheorie
(Computational Number Theory).

The course (2 hours lecture + 2 hours problem sessions, 6CP) can be given in English if participants wish so.
An announcement in English is at:
`www.math.uni-sb.de/ag/schulze/compnumber_14_english.pdf`.

Die Vorlesung wird sich mit den wichtigsten Algorithmen der elementaren Zahlentheorie beschäftigen, insbesondere mit Primzahltests und Verfahren zur Bestimmung der Primfaktorzerlegung natürlicher Zahlen sowie den analogen Problemen für Polynome über endlichen Körpern. Ferner werden grundlegende Algorithmen für das Rechnen mit Kongruenzen und in primen Restklassengruppen (u. a. diskreter Logarithmus) behandelt sowie Algorithmen zum Rechnen in Gittern, etwa der LLL-Algorithmus.
Voraussetzungen: Lineare Algebra I oder Mathematik für Informatiker, Grundkenntnisse in elementarer Zahlentheorie sind hilfreich, werden aber jeweils kurz wiederholt, wo benötigt. Die Vorlesung ist eine weiterführende Vorlesung im Bereich Algebra/Zahlentheorie, sie wendet sich an Studierende der Mathematik (Bachelor/Lehramt) und an mathematisch interessierte Studierende der Informatik.
Literatur: (Weitere Literatur in der Vorlesung)

- H. Cohen: A course in Computational Algebraic Number Theory
- R. Crandall, C. Pomerance: Prime Numbers: A computational perspective
- V. Shoup: A computational introcuction to number theory and algebra

Prof. R. Schulze-Pillot