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

In the winter semester 2014/15 I will teach a course on

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 german is at:
`www.math.uni-sb.de/ag/schulze/compnumber_14_deutsch.pdf`.

We will deal with a selection of algorithms for problems of elementary number theory, in particular primality tests and prime factoring algorithms. Algorithms for computing with congruences and in prime residue class groups (discrete logarithm problem), and for computing in lattices (LLL-algorithm) will also be treated.
Prerequisites: Linear algebra or Mathematik für Informatiker. Some elementary number theory is useful, but the relevant topics will be briefly summarized in the course. The course is intended both for students of mathematics and for mathematically interested students of Informatik.
Literature:

- 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