

Course Description of PhD course: “Finite Fields”

Credits: 2 ECTS.

Schedule: 10, 12, 14, 17, 19, 21 of December 2012, 8:15-12:00.

Lecturers: Associate professor Olav Geil and assistant professor Diego Ruano, both Department of Mathematical Sciences, Aalborg University.

Content: The origin of the theory of finite fields reaches back to the 17th and 18th centuries where fields of prime order were studied by Fermat, Euler, Lagrange, Legendre and others. General finite fields were considered by Gauss, Galois and others in the 18th century. The recent revolution of digital communication has boosted the interest in finite fields. Today the development of finite field theory is often done in an interplay with the development of applications. In this course we shall deal with the basic theory of finite fields as well as some of its applications.

Among the things we plan to cover are

- Construction of finite fields, implementation in a computer algebra system (Sage or similar).
- Polynomial functions.
- Irreducible polynomials, Conway polynomials, Berlekamp’s algorithm.
- Linearized polynomials.
- Applications: Kötter-Kschischang codes for networks, steganography, secret sharing.

Form: Six sessions of length a half day. A session consists of lectures as well as exercises.

Requirement to pass: Participation in at least five sessions. Presentation of selected exercises.