## Oberwolfach Seminar 1247b, November 18-24, 2012

# Algorithms for complex multiplication over finite fields

**Andreas Enge, Bordeaux**
**Hendrik Lenstra, Leiden**
**Peter Stevenhagen, Leiden**

## Short description

Finite fields and elliptic curves play key roles in areas of mathematics as diverse as abstract algebraic geometry and modern cryptography.
Algorithms for working with them are accordingly of critical importance to both the theoretically and the practically inclined researcher. The emphasis of the present seminar is on those algorithmic questions that are of genuine mathematical interest and seriously challenge our understanding. Part of the course addresses the efficient construction of standard models for finite fields, for potential use in computer algebra systems. Another part is concerned with the construction of elliptic curves over finite fields with given properties, as suggested by requirements from cryptography. The algorithms used for these purposes draw upon a surprisingly broad range of mathematical techniques, including class field theory and the classical theory of complex multiplication.

## Prerequisites

Mathematical maturity appropriate for a postgraduate course, including a working knowledge of the following subjects: basic algebra, Galois theory, algebraic number theory, complex function theory, analysis of algorithms, and the rudiments of elliptic curves.

## Suggested reading

David A. Cox, Primes of the form $x^2+ny^2$, Wiley, 1989.
Joseph H. Silverman, John Tate, Rational points on elliptic curves, Springer, 1992.

## Schedule

Three one-hour lectures each morning, first half of the afternoon free for doing homework, late in the afternoon discussion sections. Wednesday afternoon is free.