Algebraic number theory for the number field sieve

Jana Sotáková

April 1, 2015

Abstract

In this talk we will introduce the classic algebraic number theory required for the understanding of the algebraic computations used for the number fields sieve. Given a finite field extension $K/\mathbb{Q}$, we will mostly study the properties of the algebraic closure $\mathfrak{O}_K$ of $\mathbb{Z}$ in K. We will be most interested in dealing with the problems that arise as a result of the lack of unique factorization.

We will develop divisibility theory for ideals rather than for elements, study the unit group and also outline the practical generalizations, such as not working in the full ring of integers, which are essential for the utility of the number field sieve.