
JEAN-FRANCOIS BIASSE, University of Calgary

Sieving methods for ideal class group and unit group computation

The purpose of this talk is to give an overview of the impact of sieving methods on the computation of the ideal class group and the unit group of a number field.

Class group and unit group computation are essential tasks in computational number theory. In particular, they occur in the resolution of Diophantine equations and in the test of many unproven number theoretic conjectures.

Class group and unit group computation for number fields of small degree can be speeded up greatly by the use of sieving algorithms. We will describe how sieving methods originally developed for factoring large numbers can be adapted for our purposes and report experiments showing that this provides a significant speed-up.