AN ALGORITHM FOR VERIFYING THE p-PART OF THE CLASS GROUP

Claus Fieker and Yinan Zhang

Abstract. The class group of a number field F is an important invariant of the field and the ability to compute it is of vital importance in many parts of number theory. Unfortunately, existing methods to deliver a provable result are either slow or dependent on the Generalised Riemann Hypothesis. However, there are circumstances in Iwasawa theory and elliptic curves where only the p-part of the class group is required.

We propose an algorithm to compute the p-part of the class number of F with two different approaches, provided F is totally real and an abelian extension of the rational field $\mathbb{Q}$, for any prime p. For fields of degree 4 or higher, this algorithm is theoretically faster than classical algorithms that compute the entire class number with improvement increasing with larger field degrees.