

Un algorithme de résolution des équations quadratiques en dimension 5 sans factorisation

Pierre Castel

7 octobre 2011

Cette thèse en théorie algorithmique des nombres présente un nouvel algorithme probabiliste pour résoudre des équations quadratiques sur \mathbb{Z} ou \mathbb{Q} en dimension 5 sans utiliser de factorisation. Il est d'une complexité nettement meilleure que les algorithmes existant pour résoudre ce genre d'équations et repose sur deux algorithmes : celui de Simon et celui de Pollard et Schnorr. Après quelques rappels sur la théorie des formes quadratiques, on explique comment fonctionne cet algorithme. La suite consiste en l'analyse détaillée de cet algorithme pour laquelle on utilisera une version effective du théorème de densité de Tchebotarev.