Curve ellittiche nella rappresentazione di interi tramite forme quadratiche binarie.

Federico Pintore

Abstract

Il classico problema della risoluzione delle equazioni diofantine quadratiche include quello della rappresentazione di interi mediante forme quadratiche binarie. Quest'ultimo è risolto da un algoritmo di Gauss il quale, in generale, è di complessità computazionale esponenziale. In questo seminario si mostra che, utilizzando la connessione tra curve ellittiche e forme quadratiche binarie, il problema della rappresentazione di numeri primi può essere risolto con complessità computazionale polinomiale pur rimanendo, nel caso generale, di complessità non polinomiale la rappresentazioni di interi non primi, in quanto essa implica la fattorizzazione. In particolare, per forme quadratiche con discriminante negativo, si proporrà una soluzione alternativa a quella di Gauss, legata alle problematiche dell'Hilbert Class Field.