

Number Fields with Non-Cyclic Class Groups

J. Love
(Stanford University)

November 8, 2019

Abstract

One consequence of the Cohen-Lenstra heuristics is that for any finite abelian group A , there are infinitely many imaginary quadratic fields (IQFs) for which the class group has a subgroup isomorphic to A . While analytic techniques can check the corresponding statement for class numbers (i.e. for any n , there are infinitely many IQFs with class number divisible by n , proved by Ankeny and Chowla in 1953), it is more difficult to distinguish between groups of the same size. This talk will discuss a technique due to Mestre (1983) which constructs explicit infinite families of IQFs with a copy of $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$ in their class groups, for $p = 3, 5, 7$. The construction uses an isogeny between two elliptic curves: given a point P on the codomain, defined over some imaginary quadratic field K , we will show (under appropriate assumptions) that the preimage of P will be defined over a subfield of the Hilbert class field of K .