CORR 2000-08

Smooth Ideals in Hyperelliptic Function Fields

Andreas Enge* & Andreas Stein

Abstract Recently, several algorithms have been suggested for solving the discrete logarithm problem in the Jacobians of high-genus hyperelliptic curves over finite fields. Some of them have a provable subexponential running time and are using the fact that smooth reduced ideals are sufficiently dense. We explicitly show how these density results can be derived. All proofs are purely combinatorial and do not exploit analytic properties of generating functions.