SIEVING IN FUNCTION FIELDS

RALF FLASSENBERG AND SACHAR PAULUS

ABSTRACT. We present the first implementation of sieving techniques in the context of function fields. More precisely, we compute in class groups of quadratic congruence function fields by combining the algorithm of Hafner and McCurley with sieving ideas known from factoring. We apply our methods to the computation of generators and relations of the Jacobian variety of hyperelliptic curves over finite fields.

The algorithms introduced here were implemented in C++ with the help of LEDA and LiDIA. We provide examples of running times and comparisons with earlier algorithms.