FINDING THE EIGENVALUE IN ELKIES' ALGORITHM

MARKUS MAURER AND VOLKER MÜLLER

ABSTRACT. One essential part of Elkies' algorithm for computing the group order of an elliptic curve defined over a finite field is the determination of the eigenvalue of the Frobenius endomorphism. Here we compare from a practical point of view several strategies for this search: the use of rational functions, the use of division polynomials, the babystep-giantstep method, and a new modification of this method that avoids the need for two fast exponentiations.