ICM-9109-13 Practical Factorization of Univariate Polynomials Over Finite Fields, Vilmar Trevisan and Paul Wang.

ABSTRACT: Research presented here is part of an effort to establish state-of-the-art factoring routines for polynomials. The foundation of such algorithms lies in the efficient factorization over a finite field $GF(p^k)$. The Cantor-Zassenhaus algorithm together with innovative ideas suggested by others is compared with the Berlekamp algorithm. The studies led us to design a hybrid algorithm that combine the strengths of the different approaches. The algorithms are also implemented and machine timings are obtained to measure the performance of these algorithms.