L. BRUCE RICHMOND, University of Waterloo, Waterloo, ON

Baby-Steps Giant-Steps in Polynomial Factorization

The average cost of baby-step/giant-step polynomial factoring algorithms is considered. The distribution of the degrees of the irreducible factors of a random polynomial of degree n is relevant. Consider a partition of $[1, 2, \ldots, n]$ into intervals. Intervals that contain more than one irreducible factor degree are called *multi-factor intervals*. The fastest algorithms so far separate the product of all the irreducible factors of the polynomial with degrees belonging to a given interval from the other factors. If the interval is not multi-factor there is no need of further computation for this interval. If the interval is multifactor the product of the irreducible polynomials with degrees in the interval is computed. One expects to have more factors of lower degrees than higher degrees. One considers therefore partitions with growing interval sizes. The best partitions are what we look for. This was done for polynomials over F_2 by von zur Gauthen and Gerhard. The approach we follow uses generating functions and the asymptotics of their coefficients.