Factoring Polynomials Modulo Composites

Adam R. Klivans

May 1997
CMU-CS-97-136

School of Computer Science
Carnegie Mellon University
Pittsburgh, PA 15213

Submitted in partial fulfillment of the requirements for the degree of Master of Science (Honors Degree Program). Department of Mathematics, Carnegie Mellon University.

Abstract

Motivated by questions in circuit complexity, this paper characterizes all the factorizations of a polynomial with coefficients in the ring Z_n where n is a composite number. We give algorithms to compute such factorizations along with algebraic classifications.

Keywords: Computational algebra, Circuit complexity theory, factoring polynomials