Poster Presentation P17

TESTING BINARY POLYNOMIALS FOR IRREDUCIBILITY

Steven Hayman and Andrew Shallue*
Mathematics Department, Illinois Wesleyan University

A binary trinomial is a polynomial with three terms whose coefficients are either zero or one. A polynomial is irreducible if it does not have any nontrivial factors. Irreducible binary trinomials have a number of cryptographic and hardware applications. We have tested close to 5 billion binary polynomials for irreducibility. This computation was the result of combining various techniques from the literature.