CORR 2000-03

A Note on Shanks's Chains of Primes

E. Teske & H.C. Williams

Abstract For integers a and b we define the Shanks chain $p_1, p_2, \ldots, p_k$ of length k to be a sequence of k primes such that $p_{i+1} = ap_i^2 - b$ for $i = 1, 2, \ldots, k-1$. While for Cunningham chains it is conjectured that infinitely long chains exist, this is, in general, not true for Shanks chains. In fact, with $s = ab$ we show that for all but 56 values of $s \leq 1000$ any corresponding Shanks chain must have finite length. For this, we study certain properties of functional digraphs of quadratic functions over prime fields, both in theory and practice. We give efficient algorithms to investigate these properties and present a selection of our experimental results.