ON THE PERIODS OF GENERALIZED FIBONACCI RECURRENCES

RICHARD P. BRENT

Abstract

We give a simple condition for a linear recurrence (mod 2^w) of degree r to have the maximal possible period $2^{w-1}(2^r - 1)$. It follows that the period is maximal in the cases of interest for pseudo-random number generation, i.e. for 3-term linear recurrences defined by trinomials which are primitive (mod 2) and of degree $r > 2$. We consider the enumeration of certain exceptional polynomials which do not give maximal period, and list all such polynomials of degree less than 15.

Comments

Only the Abstract is given here. The full paper appeared as [2]. The result has applications to uniform random number generators with good statistical properties and extremely long periods [1].

References

[1] R. P. Brent, "Uniform random number generators for supercomputers", *Proc. Fifth Australian Supercomputer Conference*, Melbourne, December 1992, 95–104. ISBN 0-86444-270-X. rpb132.
[2] R. P. Brent, "On the periods of generalized Fibonacci recurrences", *Mathematics of Computation* 63 (1994), 389-401. Also appeared as Report TR-CS-92-03, Computer Sciences Laboratory, ANU, March 1992; and Report CMA-MR8-92/SMS-31-92, Centre for Mathematics and its Applications, April 1992, 11 pp. rpb133.

Computer Sciences Laboratory, Australian National University, Canberra
E-mail address: `rpb@cslab.anu.edu.au`

1991 *Mathematics Subject Classification.* Primary 11Y55, 12E05, 05A15; Secondary 11-04, 11T06, 11T55, 12-04, 12E10, 65C10, 68R05.

Key words and phrases. Fibonacci sequence, generalized Fibonacci sequence, irreducible trinomial, linear recurrence, maximal period, periodic integer sequence, primitive trinomial, pseudo-random numbers.

rpb133a typeset using $\mathcal{A}\mathcal{M}\mathcal{S}$-LaTeX.