Lucasian Primality Criteria for Specific Classes of Numbers of the Form k2^n-1

Predrag Terzic
Podgorica , Montenegro

pedja.terzic@yahoo.com

June 16, 2013

Abstract : Polynomial time prime testing algorithms for specific classes of numbers of the form k2^n-1 are introduced .
Keywords : Primality test , Riesel numbers
AMS Classification :11A51

1 Introduction

In number theory the Lucas-Lehmer-Riesel test [2] , is the fastest deterministic primality test for numbers of the form $k \cdot 2^n - 1$ with $k < 2^n$. The test was developed by Hans Riesel and it is based on Lucas-Lehmer test [1] .In this note we present how to choose starting seed for this test in case when k is divisible by 3 .

2 Main result

Conjecture 1 :
Let $N = k \cdot 2^n - 1$, such that $n > 2$, $3 \mid k$, $k < 2^n$ and
$k \equiv 1 \pmod{10}, with\ n \equiv 2,3 \pmod{4}\ or$
$k \equiv 3 \pmod{10}, with\ n \equiv 0,3 \pmod{4}\ or$
$k \equiv 7 \pmod{10}, with\ n \equiv 1,2 \pmod{4}\ or$
$k \equiv 9 \pmod{10}, with\ n \equiv 0,1 \pmod{4}$
Next , define sequence S_i :

$S_i = S_{i-1}^2 - 2$ with $S_0 = P_k(3)$
where $P_m(x) = 2^{-m} \cdot \left(\left(x - \sqrt{x^2-4}\right)^m + \left(x + \sqrt{x^2-4}\right)^m\right)$
, then
N is a prime iff $S_{n-2} \equiv 0 \pmod{N}$.

Conjecture 2
Let $N = k \cdot 2^n - 1$, such that $n > 2$, $3 \mid k$, $k < 2^n$ and
$k \equiv 3 \pmod{42}, \textit{with } n \equiv 0,2 \pmod{3} \textit{ or}$
$k \equiv 9 \pmod{42}, \textit{with } n \equiv 0 \pmod{3} \textit{ or}$
$k \equiv 15 \pmod{42}, \textit{with } n \equiv 1 \pmod{3} \textit{ or}$
$k \equiv 27 \pmod{42}, \textit{with } n \equiv 1,2 \pmod{3} \textit{ or}$
$k \equiv 33 \pmod{42}, \textit{with } n \equiv 0,1 \pmod{3} \textit{ or}$
$k \equiv 39 \pmod{42}, \textit{with } n \equiv 2 \pmod{3}$
Next , define sequence S_i :
$S_i = S_{i-1}^2 - 2$ with $S_0 = P_k(5)$
where $P_m(x) = 2^{-m} \cdot \left(\left(x - \sqrt{x^2-4}\right)^m + \left(x + \sqrt{x^2-4}\right)^m\right)$
, then
N is a prime iff $S_{n-2} \equiv 0 \pmod{N}$.

References

[1] Crandall, Richard; Pomerance, Carl (2001), "Section 4.2.1: The Lucas-Lehmer test", Prime Numbers: A Computational Perspective (1st ed.), Berlin: Springer, p. 167-170
[2] Riesel, Hans (1969). "Lucasian Criteria for the Primality of $N = h \cdot 2^n - 1$". Mathematics of Computation (American Mathematical Society) 23 (108): 869-875