A Modification of Riesel Primality Test

Predrag Terzić

Novi Sad , Serbia

e-mail: `pedja.terzic@hotmail.com`

October 09 , 2014

Abstract: Conjectured polynomial time primality test for specific class of numbers of the form $k \cdot 2^n - 1$ is introduced .

Keywords: Primality test , Polynomial time , Prime numbers .

AMS Classification: 11A51 .

1 Introduction

In 1969 Hans Riesel provided polynomial time primality test for numbers of the form $k \cdot 2^n - 1$ with k odd , $k < 2^n$ and $n > 2$, see Theorem 5 in [1] . In this note I present modified Riesel primality test that is faster in some cases than original Riesel test .

2 The Main Result

Definition 2.1. Let $P_m(x) = 2^{-m} \cdot \left(\left(x - \sqrt{x^2-4}\right)^m + \left(x + \sqrt{x^2-4}\right)^m \right)$, where m and x are nonnegative integers .

Conjecture 2.1. *Let $N = k \cdot 2^n - 1$ such that $n > 2$, k odd , $3 \nmid k$, $k < 2^n$, and f is proper factor of $n-2$.*

$$\textit{Let } S_i = P_{2^f}(S_{i-1}) \textit{ with } S_0 = P_k(4) \textit{ , thus}$$
$$N \textit{ is prime iff } S_{(n-2)/f} \equiv 0 \pmod{N}$$

Remark 2.1. Speed comparison between Maxima implementation of modified test and Maxima implementation of original Riesel test :

For $f = 2$ modified primality test is approximately faster 1.8 times than original test .

For $f = 3$ modified primality test is approximately faster 2 times than original test .

For $f = 4$ modified primality test is approximately faster 1.5 times than original test .

For $f = 5, 6 ...$ modified primality test is slower than original test .

References

[1] Riesel, Hans (1969) , ”Lucasian Criteria for the Primality of $N = h \cdot 2^n - 1$” , *Mathematics of Computation* (AmericanMathematical Society), 23 (108): 869-875 .