Notes on Number Theory and Discrete Mathematics
ISSN 1310–5132
Vol. 20, 2014, No. 5, 40–43

Conjectured polynomial time primality tests for numbers of special forms

Predrag Terzić

Podgorica, Montenegro
e-mail: pedja.terzic@hotmail.com

Abstract: Conjectured polynomial time primality tests for numbers of special forms similar to the Riesel primality test for numbers of the form $k \cdot 2^n - 1$ are introduced.
Keywords: Primality test, Polynomial time, Prime numbers.
AMS Classification: 11A51.

1 Introduction

In number theory the Riesel primality test [1], is the fastest deterministic primality test for numbers of the form $k \cdot 2^n - 1$ with k odd and $k < 2^n$. The test was developed by Hans Riesel and it is based on Lucas-Lehmer test [2]. In this note I present polynomial time primality tests that are similar to the Riesel primality test.

2 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 positive integers.

Conjecture 2.1. *Let $N = k \cdot 2^n - 1$ such that $n > 2$, $3 \mid k$, $k < 2^n$ and*

$$\begin{cases} k \equiv 1 \pmod{10} \; with \; n \equiv 2,3 \pmod 4 \\ k \equiv 3 \pmod{10} \; with \; n \equiv 0,3 \pmod 4 \\ k \equiv 7 \pmod{10} \; with \; n \equiv 1,2 \pmod 4 \\ k \equiv 9 \pmod{10} \; with \; n \equiv 0,1 \pmod 4 \end{cases}$$

Let $S_i = P_2(S_{i-1})$ *with* $S_0 = P_k(3)$*, then*
N *is prime iff* $S_{n-2} \equiv 0 \pmod{N}$

Conjecture 2.2. *Let* $N = k \cdot 2^n - 1$ *such that* $n > 2$*,* $3 \mid k$*,* $k < 2^n$ *and*

$$\begin{cases} k \equiv 3 \pmod{42} \; with \; n \equiv 0, 2 \pmod{3} \\ k \equiv 9 \pmod{42} \; with \; n \equiv 0 \pmod{3} \\ k \equiv 15 \pmod{42} \; with \; n \equiv 1 \pmod{3} \\ k \equiv 27 \pmod{42} \; with \; n \equiv 1, 2 \pmod{3} \\ k \equiv 33 \pmod{42} \; with \; n \equiv 0, 1 \pmod{3} \\ k \equiv 39 \pmod{42} \; with \; n \equiv 2 \pmod{3} \end{cases}$$

Let $S_i = P_2(S_{i-1})$ *with* $S_0 = P_k(5)$*, then*
N *is prime iff* $S_{n-2} \equiv 0 \pmod{N}$

Conjecture 2.3. *Let* $N = k \cdot 2^n + 1$ *such that* $n > 2$*,* $k < 2^n$ *and*

$$\begin{cases} k \equiv 5, 19 \pmod{42} \; with \; n \equiv 0 \pmod{3} \\ k \equiv 13, 41 \pmod{42} \; with \; n \equiv 1 \pmod{3} \\ k \equiv 17, 31 \pmod{42} \; with \; n \equiv 2 \pmod{3} \\ k \equiv 23, 37 \pmod{42} \; with \; n \equiv 0, 1 \pmod{3} \\ k \equiv 11, 25 \pmod{42} \; with \; n \equiv 0, 2 \pmod{3} \\ k \equiv 1, 29 \pmod{42} \; with \; n \equiv 1, 2 \pmod{3} \end{cases}$$

Let $S_i = P_2(S_{i-1})$ *with* $S_0 = P_k(5)$*, then*
N *is prime iff* $S_{n-2} \equiv 0 \pmod{N}$

Conjecture 2.4. *Let* $N = k \cdot 2^n + 1$ *such that* $n > 2$*,* $k < 2^n$ *and*

$$\begin{cases} k \equiv 1 \pmod{6} \; and \; k \equiv 1, 7 \pmod{10} \; with \; n \equiv 0 \pmod{4} \\ k \equiv 5 \pmod{6} \; and \; k \equiv 1, 3 \pmod{10} \; with \; n \equiv 1 \pmod{4} \\ k \equiv 1 \pmod{6} \; and \; k \equiv 3, 9 \pmod{10} \; with \; n \equiv 2 \pmod{4} \\ k \equiv 5 \pmod{6} \; and \; k \equiv 7, 9 \pmod{10} \; with \; n \equiv 3 \pmod{4} \end{cases}$$

Let $S_i = P_2(S_{i-1})$ *with* $S_0 = P_k(8)$*, then*
N *is prime iff* $S_{n-2} \equiv 0 \pmod{N}$

Conjecture 2.5. *Let* $F = 2^{2^n} + 1$ *such that* $n \geq 2$*. Let* $S_i = P_4(S_{i-1})$ *with* $S_0 = 8$*, then*

F *is prime iff* $S_{2^{n-1}-1} \equiv 0 \pmod{F}$

Conjecture 2.6. *Let* $N = k \cdot 2^n - 3$ *such that* $n > 3$*,* k *is odd* $k < 2^n$*.*

Let $S_i = P_2(S_{i-1})$ *with* $S_0 = P_k(6)$*, then*
N *is prime iff* $S_{n-1} \equiv -P_1(6) \pmod{N}$

Conjecture 2.7. *Let $N = k \cdot 2^n + 3$ such that $n > 4$, k is odd $k < 2^n$.*

$$\text{Let } S_i = P_2(S_{i-1}) \text{ with } S_0 = P_k(6), \text{ then}$$
$$N \text{ is prime iff } S_{n-1} \equiv -P_2(6) \pmod N$$

Conjecture 2.8. *Let $N = k \cdot 2^n - 5$ such that $n > 4$, k is odd $k < 2^n$.*

$$\text{Let } S_i = P_2(S_{i-1}) \text{ with } S_0 = P_k(6), \text{ then}$$
$$N \text{ is prime iff } S_{n-1} \equiv -P_2(6) \pmod N$$

Conjecture 2.9. *Let $N = k \cdot 2^n + 5$ such that $n > 4$, k is odd, $3 \nmid k$, $k < 2^n$.*

$$\text{Let } S_i = P_2(S_{i-1}) \text{ with } S_0 = P_k(4), \text{ then}$$
$$N \text{ is prime iff } S_{n-1} \equiv -P_2(4) \pmod N$$

Conjecture 2.10. *Let $N = k \cdot 2^n - 7$ such that $n > 8$, k is odd, $k < 2^n$.*

$$\text{Let } S_i = P_2(S_{i-1}) \text{ with } S_0 = P_k(6), \text{ then}$$
$$N \text{ is prime iff } S_{n-1} \equiv P_4(6) \pmod N$$

Conjecture 2.11. *Let $N = k \cdot 2^n + 7$ such that $n > 6$, k is odd, $k < 2^n$.*

$$\text{Let } S_i = P_2(S_{i-1}) \text{ with } S_0 = P_k(6), \text{ then}$$
$$N \text{ is prime iff } S_{n-1} \equiv P_3(6) \pmod N$$

Conjecture 2.12. *Let $N = k \cdot 2^n - 9$ such that $n > 5$, $k < 2^n$ and*

$$\begin{cases} k \equiv 1 \pmod 6 \; with \; n \equiv 0 \pmod 2 \\ k \equiv 5 \pmod 6 \; with \; n \equiv 1 \pmod 2 \end{cases}$$

$$\text{Let } S_i = P_2(S_{i-1}) \text{ with } S_0 = P_k(4), \text{ then}$$
$$N \text{ is prime iff } S_{n-1} \equiv -P_4(4) \pmod N$$

Conjecture 2.13. *Let $N = k \cdot 2^n + 9$ such that $n > 10$, k is odd, $k < 2^n$.*

$$\text{Let } S_i = P_2(S_{i-1}) \text{ with } S_0 = P_k(6), \text{ then}$$
$$N \text{ is prime iff } S_{n-1} \equiv P_4(6) \pmod N$$

Conjecture 2.14. *Let $N = k \cdot b^n - 1$ such that $n > 2$, k is odd, $3 \nmid k$, b is even, $3 \nmid b$, $k < b^n$.*

$$\text{Let } S_i = P_b(S_{i-1}) \text{ with } S_0 = P_{bk/2}(P_{b/2}(4)), \text{ then}$$
$$N \text{ is prime iff } S_{n-2} \equiv 0 \pmod N$$

Conjecture 2.15. *Let $N = k \cdot b^n + 1$ such that $n > 2$,b is even, $3 \nmid b$, $7 \nmid b$, $k < b^n$ and*

$$\begin{cases} k \equiv 5, 19 \pmod{42} \; with \; n \equiv 0 \pmod 3 \\ k \equiv 13, 41 \pmod{42} \; with \; n \equiv 1 \pmod 3 \\ k \equiv 17, 31 \pmod{42} \; with \; n \equiv 2 \pmod 3 \\ k \equiv 23, 37 \pmod{42} \; with \; n \equiv 0, 1 \pmod 3 \\ k \equiv 11, 25 \pmod{42} \; with \; n \equiv 0, 2 \pmod 3 \\ k \equiv 1, 29 \pmod{42} \; with \; n \equiv 1, 2 \pmod 3 \end{cases}$$

$$\text{Let } S_i = P_b(S_{i-1}) \text{ with } S_0 = P_{bk/2}(P_{b/2}(5)), \text{ then}$$
$$N \text{ is prime iff } S_{n-2} \equiv 0 \pmod{N}$$

Conjecture 2.16. *Let $N = k \cdot b^n + 1$ such that $n > 2$,b is even, $3 \nmid b$, $5 \nmid b$, $k < b^n$ and*

$$\begin{cases} k \equiv 1 \pmod{6} \; and \; k \equiv 1,7 \pmod{10} \; with \; n \equiv 0 \pmod{4} \\ k \equiv 5 \pmod{6} \; and \; k \equiv 1,3 \pmod{10} \; with \; n \equiv 1 \pmod{4} \\ k \equiv 1 \pmod{6} \; and \; k \equiv 3,9 \pmod{10} \; with \; n \equiv 2 \pmod{4} \\ k \equiv 5 \pmod{6} \; and \; k \equiv 7,9 \pmod{10} \; with \; n \equiv 3 \pmod{4} \end{cases}$$

$$\text{Let } S_i = P_b(S_{i-1}) \text{ with } S_0 = P_{bk/2}(P_{b/2}(8)), \text{ then}$$
$$N \text{ is prime iff } S_{n-2} \equiv 0 \pmod{N}$$

Conjecture 2.17. *Let $N = b^n - b - 1$ such that $n > 2$, $b \equiv 0, 6 \pmod{8}$.*

$$\text{Let } S_i = P_b(S_{i-1}) \text{ with } S_0 = P_{b/2}(6), \text{ then}$$
$$N \text{ is prime iff } S_{n-1} \equiv P_{(b+2)/2}(6) \pmod{N}$$

Conjecture 2.18. *Let $N = b^n - b - 1$ such that $n > 2$, $b \equiv 2, 4 \pmod{8}$.*

$$\text{Let } S_i = P_b(S_{i-1}) \text{ with } S_0 = P_{b/2}(6), \text{ then}$$
$$N \text{ is prime iff } S_{n-1} \equiv -P_{b/2}(6) \pmod{N}$$

Conjecture 2.19. *Let $N = b^n + b + 1$ such that $n > 2$, $b \equiv 0, 6 \pmod{8}$.*

$$\text{Let } S_i = P_b(S_{i-1}) \text{ with } S_0 = P_{b/2}(6), \text{ then}$$
$$N \text{ is prime iff } S_{n-1} \equiv P_{b/2}(6) \pmod{N}$$

Conjecture 2.20. *Let $N = b^n + b + 1$ such that $n > 2$, $b \equiv 2, 4 \pmod{8}$.*

$$\text{Let } S_i = P_b(S_{i-1}) \text{ with } S_0 = P_{b/2}(6), \text{ then}$$
$$N \text{ is prime iff } S_{n-1} \equiv -P_{(b+2)/2}(6) \pmod{N}$$

References

[1] Riesel, H. Lucasian Criteria for the Primality of $N = h \cdot 2^n - 1$, *Mathematics of Computation* (American Mathematical Society), Vol. 23(108), 1969, 869–875.

[2] Crandall, R., C. Pomerance. "Section 4.2.1: The Lucas-Lehmer test", *Prime Numbers: A Computational Perspective* (1st ed.), Berlin: Springer, 2001, 167–170.