

Conjectured Primality and Compositeness Tests for Numbers of Special Forms

Predrag Terzić

Podgorica , Montenegro

e-mail: pedja.terzic@hotmail.com

August 20 , 2014

Abstract: Conjectured polynomial time primality and compositeness tests for numbers of special forms are introduced .

Keywords: Primality test , Compositeness 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 1960 Kusta Inkeri provided unconditional , deterministic , lucasian type primality test for Fermat numbers [3] . In 2008 Ray Melham provided unconditional , probabilistic , lucasian type primality test for generalized Mersenne numbers [4] . In 2010 Pedro Berrizbeitia , Florian Luca and Ray Melham provided polynomial time compositeness test for numbers of the form $(2^p + 1)/3$, see Theorem 2 in [5] . In this note I present lucasian type primality and compositeness tests for numbers of special forms .

2 The Main Result

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

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

Let $S_i = P_2(S_{i-1})$ with $S_0 = P_k(3)$, thus
 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

$$\left\{ \begin{array}{l} k \equiv 3 \pmod{42} \text{ with } n \equiv 0, 2 \pmod{3} \\ k \equiv 9 \pmod{42} \text{ with } n \equiv 0 \pmod{3} \\ k \equiv 15 \pmod{42} \text{ with } n \equiv 1 \pmod{3} \\ k \equiv 27 \pmod{42} \text{ with } n \equiv 1, 2 \pmod{3} \\ k \equiv 33 \pmod{42} \text{ with } n \equiv 0, 1 \pmod{3} \\ k \equiv 39 \pmod{42} \text{ with } n \equiv 2 \pmod{3} \end{array} \right.$$

Let $S_i = P_2(S_{i-1})$ with $S_0 = P_k(5)$, thus
 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

$$\left\{ \begin{array}{l} k \equiv 5, 19 \pmod{42} \text{ with } n \equiv 0 \pmod{3} \\ k \equiv 13, 41 \pmod{42} \text{ with } n \equiv 1 \pmod{3} \\ k \equiv 17, 31 \pmod{42} \text{ with } n \equiv 2 \pmod{3} \\ k \equiv 23, 37 \pmod{42} \text{ with } n \equiv 0, 1 \pmod{3} \\ k \equiv 11, 25 \pmod{42} \text{ with } n \equiv 0, 2 \pmod{3} \\ k \equiv 1, 29 \pmod{42} \text{ with } n \equiv 1, 2 \pmod{3} \end{array} \right.$$

Let $S_i = P_2(S_{i-1})$ with $S_0 = P_k(5)$, thus
 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

$$\left\{ \begin{array}{l} k \equiv 1 \pmod{6} \text{ and } k \equiv 1, 7 \pmod{10} \text{ with } n \equiv 0 \pmod{4} \\ k \equiv 5 \pmod{6} \text{ and } k \equiv 1, 3 \pmod{10} \text{ with } n \equiv 1 \pmod{4} \\ k \equiv 1 \pmod{6} \text{ and } k \equiv 3, 9 \pmod{10} \text{ with } n \equiv 2 \pmod{4} \\ k \equiv 5 \pmod{6} \text{ and } k \equiv 7, 9 \pmod{10} \text{ with } n \equiv 3 \pmod{4} \end{array} \right.$$

Let $S_i = P_2(S_{i-1})$ with $S_0 = P_k(8)$, thus
 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 $S_0 = 8$, thus

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

Conjecture 2.6. Let $N = k \cdot 6^n - 1$ such that $n > 2$, $k > 0$, $k \equiv 3, 9 \pmod{10}$ and $k < 6^n$

Let $S_i = P_6(S_{i-1})$ with $S_0 = P_{3k}(P_3(3))$, thus
 N is prime iff $S_{n-2} \equiv 0 \pmod{N}$

Conjecture 2.7. Let $N = k \cdot b^n - 1$ such that $n > 2$, k is odd, $3 \nmid k$, b is even, $3 \nmid b$, $5 \nmid b$,
 $k < b^n$.

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

Conjecture 2.8. Let $N = k \cdot b^n - 1$ such that $n > 2$ and

$$\begin{cases} k \equiv 3 \pmod{30} \text{ with } b \equiv 2 \pmod{10} \text{ and } n \equiv 0, 3 \pmod{4} \\ k \equiv 3 \pmod{30} \text{ with } b \equiv 4 \pmod{10} \text{ and } n \equiv 0, 2 \pmod{4} \\ k \equiv 3 \pmod{30} \text{ with } b \equiv 6 \pmod{10} \text{ and } n \equiv 0, 1, 2, 3 \pmod{4} \\ k \equiv 3 \pmod{30} \text{ with } b \equiv 8 \pmod{10} \text{ and } n \equiv 0, 1 \pmod{4} \end{cases}$$

Let $S_i = P_b(S_{i-1})$ with $S_0 = P_{bk/2}(P_{b/2}(5778))$, thus
 N is prime iff $S_{n-2} \equiv 0 \pmod{N}$

Conjecture 2.9. Let $N = k \cdot b^n - 1$ such that $n > 2$ and

$$\begin{cases} k \equiv 9 \pmod{30} \text{ with } b \equiv 2 \pmod{10} \text{ and } n \equiv 0, 1 \pmod{4} \\ k \equiv 9 \pmod{30} \text{ with } b \equiv 4 \pmod{10} \text{ and } n \equiv 0, 2 \pmod{4} \\ k \equiv 9 \pmod{30} \text{ with } b \equiv 6 \pmod{10} \text{ and } n \equiv 0, 1, 2, 3 \pmod{4} \\ k \equiv 9 \pmod{30} \text{ with } b \equiv 8 \pmod{10} \text{ and } n \equiv 0, 3 \pmod{4} \end{cases}$$

Let $S_i = P_b(S_{i-1})$ with $S_0 = P_{bk/2}(P_{b/2}(5778))$, thus
 N is prime iff $S_{n-2} \equiv 0 \pmod{N}$

Conjecture 2.10. Let $F_n(b) = b^{2^n} + 1$ such that $n > 1$, b is even, $3 \nmid b$ and $5 \nmid b$.

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

Conjecture 2.11. Let $N = k \cdot 2^n - c$ such that $n > 2c$, $k > 0$, $c > 0$ and $c \equiv 3, 5 \pmod{8}$

Let $S_i = P_2(S_{i-1})$ with $S_0 = P_k(6)$, thus
If N is prime then $S_{n-1} \equiv -P_{\lfloor c/2 \rfloor}(6) \pmod{N}$

Conjecture 2.12. Let $N = k \cdot 2^n + c$ such that $n > 2c$, $k > 0$, $c > 0$ and $c \equiv 3, 5 \pmod{8}$

Let $S_i = P_2(S_{i-1})$ with $S_0 = P_k(6)$, thus
If N is prime then $S_{n-1} \equiv -P_{\lfloor c/2 \rfloor}(6) \pmod{N}$

Conjecture 2.13. Let $N = k \cdot 2^n - c$ such that $n > 2c$, $k > 0$, $c > 0$ and $c \equiv 1, 7 \pmod{8}$

Let $S_i = P_2(S_{i-1})$ with $S_0 = P_k(6)$, thus
If N is prime then $S_{n-1} \equiv P_{\lfloor c/2 \rfloor}(6) \pmod{N}$

Conjecture 2.14. Let $N = k \cdot 2^n + c$ such that $n > 2c$, $k > 0$, $c > 0$ and $c \equiv 1, 7 \pmod{8}$

Let $S_i = P_2(S_{i-1})$ with $S_0 = P_k(6)$, thus
 If N is prime then $S_{n-1} \equiv P_{\lfloor c/2 \rfloor}(6) \pmod{N}$

Conjecture 2.15. Let $N = b^n - b - 1$ such that $n > 2$, $b \equiv 0, 6 \pmod{8}$.

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

Conjecture 2.16. Let $N = b^n - b - 1$ such that $n > 2$, $b \equiv 2, 4 \pmod{8}$.

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

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

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

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

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

References

- [1] Riesel, Hans (1969), "Lucasian Criteria for the Primality of $k \cdot 2^n - 1$ ", *Mathematics of Computation* (American Mathematical Society), 23 (108): 869-875 .
- [2] 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 .
- [3] Inkeri, K., "Tests for primality", *Ann. Acad. Sci. Fenn.*, A I 279, 119 (1960).
- [4] R. S. Melham , "Probable prime tests for generalized Mersenne numbers," , *Bol. Soc. Mat. Mexicana* , 14 (2008) , 7-14 .
- [5] Pedro Berrizbeitia ,Florian Luca ,Ray Melham , "On a Compositeness Test for $(2^p + 1)/3$ ", *Journal of Integer Sequences*, Vol. 13 (2010), Article 10.1.7 .