Probable Prime Test for Specific Class of $N = k \cdot b^n - 1$

Predrag Terzić

Bulevar Pera Ćetkovića 139 , Podgorica , Montenegro
e-mail: pedja.terzic@hotmail.com

Abstract: Polynomial time probable prime test for specific class of $N = k \cdot b^n - 1$ is introduced
Keywords: Compositeness test , Polynomial time , Prime numbers .
AMS Classification: 11A51 .

1 Introduction

In 1856 Edouard Lucas developed primality test for Mersenne numbers . The test was improved by Lucas in 1878 and Derrick Henry Lehmer in the 1930s , see [1].In 1969 Hans Riesel formulated primality test , see [2] for numbers of the form $k \cdot 2^n - 1$ with k odd and $k < 2^n$. In this note we present lucasian type compositeness test for specific class of $k \cdot b^n - 1$.

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 positive integers .

Theorem 2.1. *Let* $N = k \cdot b^n - 1$ *such that* $k > 0$,$3 \nmid k$,$b > 0$, b *is even number* , $3 \nmid b$ *and* $n > 2$ *.Let* $S_i = P_b(S_{i-1})$ *with* $S_0 = P_{kb/2}(P_{b/2}(4))$ *, thus If* N *is prime then* $S_{n-2} \equiv 0 \pmod{N}$

The following proof appeared for the first time on MSE forum in January 2017 , see [3].
Proof. Let us prove by induction that

$$S_i = p^{kb^{i+2}/4} + q^{kb^{i+2}/4}$$

where $p = 2-\sqrt{3}, q = 2+\sqrt{3}$ with $pq = 1$.

$$S_0 = P_{kb/2}(P_{b/2}(4))$$

$$= P_{kb/2}\left(p^{b/2}+q^{b/2}\right)$$

$$= 2^{-kb/2}\left(p^{b/2}+q^{b/2}-\sqrt{(p^{b/2}+q^{b/2})^2-4}\right)^{kb/2}+2^{-kb/2}\left(p^{b/2}+q^{b/2}+\sqrt{(p^{b/2}+q^{b/2})^2-4}\right)^{kb/2}$$

$$= 2^{-kb/2}\left(p^{b/2}+q^{b/2}-\left(q^{b/2}-p^{b/2}\right)\right)^{kb/2}+2^{-kb/2}\left(p^{b/2}+q^{b/2}+\left(q^{b/2}-p^{b/2}\right)\right)^{kb/2}$$

$$= p^{kb^2/4}+q^{kb^2/4}$$

Supposing that $S_i = p^{kb^{i+2}/4}+q^{kb^{i+2}/4}$ gives that

$$S_{i+1} = P_b(S_i)$$

$$= P_b(p^{kb^{i+2}/4}+q^{kb^{i+2}/4})$$

$$= 2^{-b}\left(p^{kb^{i+2}/4}+q^{kb^{i+2}/4}-\sqrt{(p^{kb^{i+2}/4}+q^{kb^{i+2}/4})^2-4}\right)^b$$

$$+2^{-b}\left(p^{kb^{i+2}/4}+q^{kb^{i+2}/4}+\sqrt{(p^{kb^{i+2}/4}+q^{kb^{i+2}/4})^2-4}\right)^b$$

$$= 2^{-b}\left(p^{kb^{i+2}/4}+q^{kb^{i+2}/4}-\left(q^{kb^{i+2}/4}-p^{kb^{i+2}/4}\right)\right)^b$$

$$+2^{-b}\left(p^{kb^{i+2}/4}+q^{kb^{i+2}/4}+\left(q^{kb^{i+2}/4}-p^{kb^{i+2}/4}\right)\right)^b$$

$$= p^{kb^{i+3}/4}+q^{kb^{i+3}/4} \qquad \blacksquare$$

Now

$$S_{n-2} = p^{(N+1)/4}+q^{(N+1)/4}$$

Squaring the both sides gives

$$S_{n-2}^2 = p^{(N+1)/2}+q^{(N+1)/2}+2 \tag{1}$$

Using that

$$\sqrt{2\pm\sqrt{3}} = \frac{\sqrt{3}\pm 1}{\sqrt{2}}$$

we get

$$
\begin{aligned}
2^{(N+1)/2}(p^{(N+1)/2}+q^{(N+1)/2}) &= (\sqrt{3}-1)^{N+1}+(\sqrt{3}+1)^{N+1} \\
&= \sum_{i=0}^{N+1}\binom{N+1}{i}(\sqrt{3})^i((-1)^{N+1-i}+1^{N+1-i}) \\
&= \sum_{j=0}^{(N+1)/2}\binom{N+1}{2j}(\sqrt{3})^{2j}\cdot 2 \\
&\equiv 2+2\cdot 3^{(N+1)/2} \pmod N \\
&\equiv 2+2\cdot(-3) \pmod N \\
&\equiv -4 \pmod N
\end{aligned}
$$

where

$$3^{(N+1)/2}=3\cdot 3^{(N-1)/2}\equiv 3\left(\frac{3}{N}\right)=3\cdot\frac{(-1)^{\frac{3-1}{2}\cdot\frac{N-1}{2}}}{\left(\frac{N}{3}\right)}=3\cdot\frac{-1}{1}=-3 \pmod N$$

Since

$$2^{(N+1)/2}=2\cdot 2^{(N-1)/2}\equiv 2\left(\frac{2}{N}\right)=2\cdot(-1)^{(N^2-1)/8}\equiv 2 \pmod N$$

is coprime to N, we get

$$p^{(N+1)/2}+q^{(N+1)/2}\equiv -2 \pmod N \tag{2}$$

It follows from $(1)(2)$ that

$$S_{n-2}\equiv 0 \pmod N$$

as desired.

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 .

[3] mathlove (http://math.stackexchange.com/users/78967/mathlove), Probable prime test for specific class of $N = k \cdot b^n - 1$, URL (version: 2017-01-30): http://math.stackexchange.com/q/2121030