Probable Prime Tests for Generalized Fermat Numbers

Predrag Terzić

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

Abstract: Polynomial time compositeness tests for generalized Fermat numbers are introduced .
Keywords: Primality test , Polynomial time , Prime numbers .
AMS Classification: 11A51 .

1 The Main Result

Definition 1.1. 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.

Theorem 1.1. *Let $F_n(b) = b^{2^n} + 1$ such that $n \geq 2$ and b is even number .*
Let $S_i = P_b(S_{i-1})$ with $S_0 = P_b(6)$, thus if $F_n(b)$ is prime, then $S_{2^n-1} \equiv 2 \pmod{F_n(b)}$.

The following proof appeared for the first time on MSE forum in August 2016 , see [1]

Proof . First of all, we prove by induction that

$$S_i = \alpha^{b^{i+1}} + \beta^{b^{i+1}} \tag{1}$$

where $\alpha = 3 - 2\sqrt{2}, \beta = 3 + 2\sqrt{2}$ with $\alpha\beta = 1$.

Proof for (1) :

$$\begin{aligned} S_0 &= P_b(6) \\ &= 2^{-b} \cdot \left(\left(6 - 4\sqrt{2}\right)^b + \left(6 + 4\sqrt{2}\right)^b \right) \\ &= 2^{-b} \cdot \left(2^b(3 - 2\sqrt{2})^b + 2^b(3 + 2\sqrt{2})^b \right) \\ &= \alpha^b + \beta^b \end{aligned}$$

Suppose that (1) holds for i. Using the fact that

$$(\alpha^m + \beta^m)^2 - 4 = (\beta^m - \alpha^m)^2$$

we get

$$
\begin{aligned}
S_{i+1} &= P_b(S_i)\\
&= 2^{-b}\cdot\left(\left(\alpha^{b^{i+1}}+\beta^{b^{i+1}}-\sqrt{(\alpha^{b^{i+1}}+\beta^{b^{i+1}})^2-4}\right)^b+\left(\alpha^{b^{i+1}}+\beta^{b^{i+1}}+\sqrt{(\alpha^{b^{i+1}}+\beta^{b^{i+1}})^2-4}\right)^b\right)\\
&= 2^{-b}\cdot\left(\left(\alpha^{b^{i+1}}+\beta^{b^{i+1}}-\sqrt{(\beta^{b^{i+1}}-\alpha^{b^{i+1}})^2}\right)^b+\left(\alpha^{b^{i+1}}+\beta^{b^{i+1}}+\sqrt{(\beta^{b^{i+1}}-\alpha^{b^{i+1}})^2}\right)^b\right)\\
&= 2^{-b}\cdot\left(\left(2\alpha^{b^{i+1}}\right)^b+\left(2\beta^{b^{i+1}}\right)^b\right)\\
&= \alpha^{b^{i+2}}+\beta^{b^{i+2}} \qquad \blacksquare
\end{aligned}
$$

Let $N := F_n(b) = b^{2^n}+1$. Then, from (1),

$$S_{2^n-1} = \alpha^{b^{2^n}}+\beta^{b^{2^n}} = \alpha^{N-1}+\beta^{N-1}$$

Since $\alpha\beta = 1$,

$$
\begin{aligned}
S_{2^n-1} &= \alpha^{N-1}+\beta^{N-1}\\
&= \alpha\beta(\alpha^{N-1}+\beta^{N-1})\\
&= \beta\cdot\alpha^N+\alpha\cdot\beta^N\\
&= 3(\alpha^N+\beta^N)-2\sqrt{2}\,(\beta^N-\alpha^N) \qquad (2)
\end{aligned}
$$

So, in the following, we find $\alpha^N+\beta^N \pmod N$ and $\sqrt{2}\,(\beta^N-\alpha^N) \pmod N$.
Using the binomial theorem,

$$
\begin{aligned}
\alpha^N+\beta^N &= (3-2\sqrt{2})^N+(3+2\sqrt{2})^N\\
&= \sum_{i=0}^{N}\binom{N}{i}3^i\cdot((-2\sqrt{2})^{N-i}+(2\sqrt{2})^{N-i})\\
&= \sum_{j=1}^{(N+1)/2}\binom{N}{2j-1}3^{2j-1}\cdot 2(2\sqrt{2})^{N-(2j-1)}
\end{aligned}
$$

Since $\binom{N}{2j-1}\equiv 0 \pmod N$ for $1\le j\le (N-1)/2$, we get

$$\alpha^N+\beta^N \equiv \binom{N}{N}3^N\cdot 2(2\sqrt{2})^0 \equiv 2\cdot 3^N \pmod N$$

Now, by Fermat's little theorem,

$$\alpha^N+\beta^N \equiv 2\cdot 3^N \equiv 2\cdot 3 \equiv 6 \pmod N \qquad (3)$$

Similarly,

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

By the way, since b is even with $n \geq 2$,

$$N = b^{2^n} + 1 \equiv 1 \pmod 8$$

from which

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

follows where $\left(\frac{q}{p}\right)$ denotes the Legendre symbol .

So, from (4),

$$\sqrt{2}\,(\beta^N - \alpha^N) \equiv 4 \cdot 2^{(N+1)/2} \equiv 4 \cdot 2 \equiv 8 \pmod N \qquad (5)$$

Therefore, finally, from $(2)(3)$ and (5),

$$S_{2^n-1} \equiv 3(\alpha^N + \beta^N) - 2\sqrt{2}\,(\beta^N - \alpha^N) \equiv 3 \cdot 6 - 2 \cdot 8 \equiv 2 \pmod{F_n(b)}$$

as desired.

Theorem 1.2. *Let $E_n(b) = \frac{b^{2^n}+1}{2}$ such that $n > 1$, b is odd number greater than one .*
Let $S_i = P_b(S_{i-1})$ with $S_0 = P_b(6)$, thus if $E_n(b)$ is prime, then $S_{2^n-1} \equiv 6 \pmod{E_n(b)}$.

The following proof appeared for the first time on MSE forum in August 2016 , see [2]

Proof . First of all, we prove by induction that

$$S_i = p^{2b^{i+1}} + q^{2b^{i+1}} \qquad (6)$$

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

Proof for (6) :

$$S_0 = P_b(6) = 2^{-b} \cdot \left(\left(6 - 4\sqrt{2}\right)^b + \left(6 + 4\sqrt{2}\right)^b\right) = (3-2\sqrt{2})^b + (3+2\sqrt{2})^b = p^{2b} + q^{2b}$$

Supposing that (6) holds for i gives

$$\begin{aligned} S_{i+1} &= P_b(S_i) \\ &= 2^{-b} \cdot \left(\left(S_i - \sqrt{S_i^2 - 4} \right)^b + \left(S_i + \sqrt{S_i^2 - 4} \right)^b \right) \\ &= 2^{-b} \cdot \left(\left(p^{2b^{i+1}} + q^{2b^{i+1}} - \sqrt{\left(q^{2b^{i+1}} - p^{2b^{i+1}}\right)^2} \right)^b + \left(p^{2b^{i+1}} + q^{2b^{i+1}} + \sqrt{\left(q^{2b^{i+1}} - p^{2b^{i+1}}\right)^2} \right)^b \right) \\ &= 2^{-b} \cdot \left(\left(p^{2b^{i+1}} + q^{2b^{i+1}} - \left(q^{2b^{i+1}} - p^{2b^{i+1}}\right) \right)^b + \left(p^{2b^{i+1}} + q^{2b^{i+1}} + \left(q^{2b^{i+1}} - p^{2b^{i+1}}\right) \right)^b \right) \\ &= 2^{-b} \cdot \left(\left(2p^{2b^{i+1}}\right)^b + \left(2q^{2b^{i+1}}\right)^b \right) \\ &= p^{2b^{i+2}} + q^{2b^{i+2}} \quad \blacksquare \end{aligned}$$

Let $N := 2^n - 1$, $M := E_n(b) = (b^{N+1} + 1)/2$. From (6), we have

$$\begin{aligned} S_{2^n-1} &= S_N \\ &= p^{2b^{N+1}} + q^{2b^{N+1}} \\ &= p^{2(2M-1)} + q^{2(2M-1)} \\ &= p^{4M-2} + q^{4M-2} \\ &= (pq)^2(p^{4M-2} + q^{4M-2}) \\ &= 3(p^{4M} + q^{4M}) - 2\sqrt{2}\,(q^{4M} - p^{4M}) \end{aligned}$$

Now using the binomial theorem and Fermat's little theorem,

$$\begin{aligned} p^{4M} + q^{4M} &= (17 - 12\sqrt{2})^M + (17 + 12\sqrt{2})^M \\ &= \sum_{i=0}^{M} \binom{M}{i} 17^i((-12\sqrt{2})^{M-i} + (12\sqrt{2})^{M-i}) \\ &= \sum_{j=1}^{(M+1)/2} \binom{M}{2j-1} 17^{2j-1} \cdot 2(12\sqrt{2})^{M-(2j-1)} \\ &\equiv \binom{M}{M} 17^M \cdot 2(12\sqrt{2})^0 \pmod{M} \\ &\equiv 17 \cdot 2 \pmod{M} \\ &\equiv 34 \pmod{M} \end{aligned}$$

Similarly,

$$\begin{aligned}
2\sqrt{2}\,(q^{4M}-p^{4M}) &= 2\sqrt{2}\,((17+12\sqrt{2})^M-(17-12\sqrt{2})^M)\\
&= 2\sqrt{2}\,\sum_{i=0}^{M}\binom{M}{i}17^i((12\sqrt{2})^{M-i}-(-12\sqrt{2})^{M-i})\\
&= 2\sqrt{2}\,\sum_{j=0}^{(M-1)/2}\binom{M}{2j}17^{2j}\cdot 2(12\sqrt{2})^{M-2j}\\
&= \sum_{j=0}^{(M-1)/2}\binom{M}{2j}17^{2j}\cdot 4\cdot 12^{M-2j}\cdot 2^{(M-2j+1)/2}\\
&\equiv \binom{M}{0}17^0\cdot 4\cdot 12^M\cdot 2^{(M+1)/2} \pmod{M}\\
&\equiv 4\cdot 12\cdot 2 \pmod{M}\\
&\equiv 96 \pmod{M}
\end{aligned}$$

since $2^{(M-1)/2} \equiv (-1)^{(M^2-1)/8} \equiv 1 \pmod{M}$ (this is because $M \equiv 1 \pmod{8}$ from $b^2 \equiv 1, 9 \pmod{16}$)

It follows from these that

$$\begin{aligned}
S_{2^n-1} &= 3(p^{4M}+q^{4M})-2\sqrt{2}\,(q^{4M}-p^{4M})\\
&\equiv 3\cdot 34-96 \pmod{M}\\
&\equiv 6 \pmod{E_n(b)}
\end{aligned}$$

as desired.

References

[1] mathlove (http://math.stackexchange.com/users/78967/mathlove), Conjectured Compositeness Test for Generalized Fermat Numbers, URL (version: 2016-08-17): http://math.stackexchange.com/q/1894774

[2] mathlove (http://math.stackexchange.com/users/78967/mathlove), Conjectured Compositeness Test for $E_n(b)=\frac{b^{2^n}+1}{2}$, URL (version: 2016-08-20): http://math.stackexchange.com/q/1897867