Research Project Primus

Predrag Terzić

e-mail: pedja.terzic@hotmail.com

April 25 , 2016

1 Compositeness tests for $N = k \cdot b^n \pm c$

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.

Conjecture 1.1.

Let $N = k \cdot b^n - c$ *such that* $b \equiv 0 \pmod 2, n > bc, k > 0, c > 0$

and $c \equiv 1, 7 \pmod 8$

Let $S_i = P_b(S_{i-1})$ *with* $S_0 = P_{bk/2}(P_{b/2}(6)),$ *thus*

If N *is prime then* $S_{n-1} \equiv P_{(b/2)\cdot\lceil c/2 \rceil}(6) \pmod N$

Conjecture 1.2.

Let $N = k \cdot b^n - c$ *such that* $b \equiv 0, 4, 8 \pmod{12}, n > bc, k > 0, c > 0$

and $c \equiv 3, 5 \pmod 8$.

Let $S_i = P_b(S_{i-1})$ *with* $S_0 = P_{bk/2}(P_{b/2}(6)),$ *thus*

If N *is prime then* $S_{n-1} \equiv P_{(b/2)\cdot\lfloor c/2 \rfloor}(6) \pmod N$

Conjecture 1.3.

Let $N = k \cdot b^n - c$ *such that* $b \equiv 2, 6, 10 \pmod{12}, n > bc, k > 0, c > 0$

and $c \equiv 3, 5 \pmod 8$.

Let $S_i = P_b(S_{i-1})$ *with* $S_0 = P_{bk/2}(P_{b/2}(6)),$ *thus*

If N *is prime then* $S_{n-1} \equiv -P_{(b/2)\cdot\lfloor c/2 \rfloor}(6) \pmod N$

Conjecture 1.4.

$$\textit{Let } N = k \cdot b^n + c \textit{ such that } b \equiv 0 \pmod 2, n > bc, k > 0, c > 0$$

$$\textit{and } c \equiv 1, 7 \pmod 8)$$

$$\textit{Let } S_i = P_b(S_{i-1}) \textit{ with } S_0 = P_{bk/2}(P_{b/2}(6)), \textit{ thus}$$

$$\textit{If } N \textit{ is prime then } S_{n-1} \equiv P_{(b/2)\cdot\lfloor c/2 \rfloor}(6) \pmod N)$$

Conjecture 1.5.

$$\textit{Let } N = k \cdot b^n + c \textit{ such that } b \equiv 0, 4, 8 \pmod{12}, n > bc, k > 0, c > 0$$

$$\textit{and } c \equiv 3, 5 \pmod 8.$$

$$\textit{Let } S_i = P_b(S_{i-1}) \textit{ with } S_0 = P_{bk/2}(P_{b/2}(6)), \textit{ thus}$$

$$\textit{If } N \textit{ is prime then } S_{n-1} \equiv P_{(b/2)\cdot\lceil c/2 \rceil}(6) \pmod N)$$

Conjecture 1.6.

$$\textit{Let } N = k \cdot b^n + c \textit{ such that } b \equiv 2, 6, 10 \pmod{12}, n > bc, k > 0, c > 0$$

$$\textit{and } c \equiv 3, 5 \pmod 8.$$

$$\textit{Let } S_i = P_b(S_{i-1}) \textit{ with } S_0 = P_{bk/2}(P_{b/2}(6)), \textit{ thus}$$

$$\textit{If } N \textit{ is prime then } S_{n-1} \equiv -P_{(b/2)\cdot\lceil c/2 \rceil}(6) \pmod N)$$

Proof attempt by mathlove

First of all,

$$\begin{aligned} P_{b/2}(6) &= 2^{-b/2}\left(\left(6-4\sqrt{2}\right)^{b/2} + \left(6+4\sqrt{2}\right)^{b/2}\right) \\ &= \left(3-2\sqrt{2}\right)^{b/2} + \left(3+2\sqrt{2}\right)^{b/2} \\ &= p^b + q^b \end{aligned}$$

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

From

$$S_0 = P_{bk/2}(P_{b/2}(6)) = 2^{-bk/2}\left(\left(2p^b\right)^{bk/2} + \left(2q^b\right)^{bk/2}\right) = p^{b^2k/2} + q^{b^2k/2}$$

and $S_i = P_b(S_{i-1})$, we can prove by induction on $i \in \mathbb{N}$ that

$$S_i = p^{b^{i+2}k/2} + q^{b^{i+2}k/2}.$$

By the way,

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

Also,

$$\begin{aligned}
p^{N+3}+q^{N+3} &= \sum_{i=0}^{N+3}\binom{N+3}{i}(\sqrt{2})^i\left((-1)^{N+3-i}+1\right)\\
&= \sum_{j=0}^{(N+3)/2}\binom{N+3}{2j}2^{j+1}\\
&\equiv 2+\binom{N+3}{2}\cdot 2^2+\binom{N+3}{N+1}\cdot 2^{\frac{N+3}{2}}+2^{\frac{N+5}{2}} \pmod N\\
&\equiv 14+12\cdot 2^{\frac{N-1}{2}}+8\cdot 2^{\frac{N-1}{2}} \pmod N
\end{aligned} \tag{2}$$

For $N\equiv \pm 1 \pmod 8$, since $2^{\frac{N-1}{2}}\equiv 1 \pmod N$, from $(1)(2)$, we can prove by induction on $i\in\mathbb{Z}$ that

$$p^{N+2i-1}+q^{N+2i-1}\equiv p^{2i}+q^{2i} \pmod N \tag{3}$$

For $N\equiv 3,5 \pmod 8$, since $2^{\frac{N-1}{2}}\equiv -1 \pmod N$, from $(1)(2)$, we can prove by induction on $i\in\mathbb{Z}$ that

$$p^{N+2i-1}+q^{N+2i-1}\equiv -\left(p^{2i-2}+q^{2i-2}\right) \pmod N \tag{4}$$

To prove $(3)(4)$, we can use

$$\begin{aligned}
p^{N+2(i+1)-1}+q^{N+2(i+1)-1} &\equiv \left(p^{N+2i-1}+q^{N+2i-1}\right)\left(p^2+q^2\right)-\\
&-\left(p^{N+2(i-1)-1}+q^{N+2(i-1)-1}\right) \pmod N
\end{aligned}$$

and

$$\begin{aligned}
p^{N+2(i-1)-1}+q^{N+2(i-1)-1} &\equiv \left(p^{N+2i-1}+q^{N+2i-1}\right)\left(p^{-2}+q^{-2}\right)-\\
&-\left(p^{N+2(i+1)-1}+q^{N+2(i+1)-1}\right) \pmod N
\end{aligned}$$

Now, for $N\equiv \pm 1 \pmod 8$, from (3), we can prove by induction on $j\in\mathbb{N}$ that

$$p^{j(N+2i-1)}+q^{j(N+2i-1)}\equiv p^{2ij}+q^{2ij} \pmod N \tag{5}$$

Also, for $N\equiv 3,5 \pmod 8$, from (4), we can prove by induction on $j\in\mathbb{N}$ that

$$p^{j(N+2i-1)}+q^{j(N+2i-1)}\equiv (-1)^j\left(p^{j(2i-2)}+q^{j(2i-2)}\right) \pmod N \tag{6}$$

To prove $(5)(6)$, we can use

$$p^{(j+1)(N+2i-1)}+q^{(j+1)(N+2i-1)} \equiv \left(p^{j(N+2i-1)}+q^{j(N+2i-1)}\right)\left(p^{N+2i-1}+q^{N+2i-1}\right)- \\ -\left(p^{(j-1)(N+2i-1)}+q^{(j-1)(N+2i-1)}\right) \pmod N$$

For conjecture 1.1, $N \equiv \pm 1 \pmod 8$ follows from the conditions $N = k \cdot b^n - c$ such that $b \equiv 0 \pmod 2, n > bc, k > 0, c > 0$ and $c \equiv 1, 7 \pmod 8$. Then, we can say that conjecture 1.1 is true because using (5) and setting $c = 2d - 1$ gives

$$\begin{aligned} S_{n-1} &= p^{b^{n+1}k/2}+q^{b^{n+1}k/2} \\ &= p^{(b/2)(N+c)}+q^{(b/2)(N+c)} \\ &= p^{(b/2)(N+2d-1)}+q^{(b/2)(N+2d-1)} \\ &\equiv p^{2\cdot d\cdot(b/2)}+q^{2\cdot d\cdot(b/2)} \pmod N \\ &\equiv P_{(b/2)\cdot d}(6) \pmod N \\ &\equiv P_{(b/2)\cdot\lceil c/2\rceil}(6) \pmod N \end{aligned}$$

Q.E.D.

For conjecture 1.2, $N \equiv 3, 5 \pmod 8$ follows from the conditions $N = k\cdot b^n - c$ such that $b \equiv 0, 4, 8 \pmod{12}, n > bc, k > 0, c > 0,$ and $c \equiv 3, 5 \pmod 8$. Then, we can say that conjecture 1.2 is true because using (6) and setting $c = 2d - 1$ gives

$$\begin{aligned} S_{n-1} &= p^{b^{n+1}k/2}+q^{b^{n+1}k/2} \\ &= p^{(b/2)(N+c)}+q^{(b/2)(N+c)} \\ &= p^{(b/2)(N+2d-1)}+q^{(b/2)(N+2d-1)} \\ &\equiv (-1)^{b/2}\left(p^{(b/2)\cdot(2d-2)}+q^{(b/2)\cdot(2d-2)}\right) \pmod N \\ &\equiv P_{(b/2)\cdot(d-1)}(6) \pmod N \\ &\equiv P_{(b/2)\cdot\lfloor c/2\rfloor}(6) \pmod N \end{aligned}$$

Q.E.D.

For conjecture 1.3, $N \equiv 3, 5 \pmod 8$ follows from the conditions $N = k\cdot b^n - c$ such that $b \equiv 2, 6, 10 \pmod{12}, n > bc, k > 0, c > 0$, and $c \equiv 3, 5 \pmod 8$. Then, we can say that conjecture 1.3 is true because using (6) and setting $c = 2d - 1$ gives

$$\begin{aligned} S_{n-1} &= p^{b^{n+1}k/2}+q^{b^{n+1}k/2} \\ &= p^{(b/2)(N+c)}+q^{(b/2)(N+c)} \\ &= p^{(b/2)(N+2d-1)}+q^{(b/2)(N+2d-1)} \\ &\equiv (-1)^{b/2}\left(p^{(b/2)\cdot(2d-2)}+q^{(b/2)\cdot(2d-2)}\right) \pmod N \\ &\equiv -P_{(b/2)\cdot(d-1)}(6) \pmod N \\ &\equiv -P_{(b/2)\cdot\lfloor c/2\rfloor}(6) \pmod N \end{aligned}$$

Q.E.D.

For conjecture 1.4, $N \equiv \pm 1 \pmod 8$ follows from the conditions $N = k \cdot b^n + c$ such that $b \equiv 0 \pmod 2, n > bc, k > 0, c > 0$ and $c \equiv 1, 7 \pmod 8$. Then, we can say that conjecture 1.4 is true because using (5) and setting $c = 2d - 1$ gives

$$\begin{aligned}
S_{n-1} &= p^{b^{n+1}k/2} + q^{b^{n+1}k/2} \\
&= p^{(b/2)(N-c)} + q^{(b/2)(N-c)} \\
&= p^{(b/2)(N-2d+1))} + q^{(b/2)(N-2d+1)} \\
&= p^{(b/2)(N+2(-d+1)-1)} + q^{(b/2)(N+2(-d+1)-1)} \\
&\equiv p^{2\cdot(-d+1)\cdot(b/2)} + q^{2\cdot(-d+1)\cdot(b/2)} \pmod N \\
&\equiv q^{2\cdot(d-1)\cdot(b/2)} + p^{2\cdot(d-1)\cdot(b/2)} \pmod N \\
&\equiv P_{(b/2)\cdot(d-1)}(6) \pmod N \\
&\equiv P_{(b/2)\cdot\lfloor c/2 \rfloor}(6) \pmod N
\end{aligned}$$

Q.E.D.

For conjecture 1.5, $N \equiv 3, 5 \pmod 8$ follows from the conditions $N = k \cdot b^n + c$ such that $b \equiv 0, 4, 8 \pmod{12}, n > bc, k > 0, c > 0$, and $c \equiv 3, 5 \pmod 8$. Then, we can say that conjecture 1.5 is true because using (6) and setting $c = 2d - 1$ gives

$$\begin{aligned}
S_{n-1} &= p^{b^{n+1}k/2} + q^{b^{n+1}k/2} \\
&= p^{(b/2)(N-c)} + q^{(b/2)(N-c)} \\
&= p^{(b/2)(N-2d+1)} + q^{(b/2)(N-2d+1)} \\
&= p^{(b/2)(N+2(-d+1)-1)} + q^{(b/2)(N+2(-d+1)-1)} \\
&\equiv (-1)^{b/2} \left(p^{(b/2)\cdot(2(-d+1)-2)} + q^{(b/2)\cdot(2(-d+1)-2)}\right) \pmod N \\
&\equiv q^{(b/2)\cdot 2d} + p^{(b/2)\cdot 2d} \pmod N \\
&\equiv P_{(b/2)\cdot d}(6) \pmod N \\
&\equiv P_{(b/2)\cdot\lceil c/2 \rceil}(6) \pmod N
\end{aligned}$$

Q.E.D.

For conjecture 1.6, $N \equiv 3, 5 \pmod 8$ follows from the conditions $N = k \cdot b^n + c$ such that $b \equiv 2, 6, 10 \pmod{12}, n > bc, k > 0, c > 0$, and $c \equiv 3, 5 \pmod 8$. Then, we can say that conjecture 1.6 is true because using (6) and setting $c = 2d - 1$ gives

$$\begin{aligned}
S_{n-1} &= p^{b^{n+1}k/2} + q^{b^{n+1}k/2} \\
&= p^{(b/2)(N-c)} + q^{(b/2)(N-c)} \\
&= p^{(b/2)(N-2d+1)} + q^{(b/2)(N-2d+1)} \\
&= p^{(b/2)(N+2(-d+1)-1)} + q^{(b/2)(N+2(-d+1)-1)} \\
&\equiv (-1)^{b/2} \left(p^{(b/2)\cdot(2(-d+1)-2)} + q^{(b/2)\cdot(2(-d+1)-2)}\right) \pmod N \\
&\equiv -\left(q^{(b/2)\cdot 2d} + p^{(b/2)\cdot 2d}\right) \pmod N \\
&\equiv -P_{(b/2)\cdot d}(6) \pmod N \\
&\equiv -P_{(b/2)\cdot\lceil c/2 \rceil}(6) \pmod N
\end{aligned}$$

Q.E.D.

2 Primality tests for specific classes of $N = k \cdot 2^m \pm 1$

Throughout this post we use the following notations: $\mathbb{Z}$-the set of integers , $\mathbb{N}$-the set of positive integers , $\left(\frac{a}{p}\right)$-the Jacobi symbol , (m,n)-the greatest common divisor of m and n , $S_n(x)$-the sequence defined by $S_0(x) = x$ and $S_{k+1}(x) = (S_k(x))^2 - 2(k \geq 0)$.

Basic Lemmas and Theorems

Definition 2.1. For $P, Q \in \mathbb{Z}$ the Lucas sequence $\{V_n(P,Q)\}$ is defined by $V_0(P,Q) = 2, V_1(P,Q) = P, V_{n+1}(P,Q) = PV_n(P,Q) - QV_{n-1}(P,Q)(n \geq 1)$ Let $D = P^2 - 4Q$. It is known that

$$V_n(P,Q) = \left(\frac{P+\sqrt{D}}{2}\right)^n + \left(\frac{P-\sqrt{D}}{2}\right)^n$$

Lemma 2.1. *Let $P, Q \in \mathbb{Z}$ and $n \in \mathbb{N}$. Then*

$$V_n(P,Q) = \sum_{r=0}^{[n/2]} \frac{n}{n-r}\binom{n-r}{r} P^{n-2r}(-Q)^r$$

Theorem 2.1. *(Zhi-Hong Sun)*

For $m \in \{2,3,4,...\}$ let $p = k \cdot 2^m \pm 1$ with $0 < k < 2^m$ and k odd . If $b, c \in \mathbb{Z}$, $(p,c) = 1$ and $\left(\frac{2c+b}{p}\right) = \left(\frac{2c-b}{p}\right) = -\left(\frac{c}{p}\right)$ then p is prime if and only if $p \mid S_{m-2}(x)$, where $x = c^{-k}V_k(b,c^2) = \sum_{r=0}^{(k-1)/2} \frac{k}{k-r}\binom{k-r}{r}(-1)^r(b/c)^{k-2r}$

Lemma 2.2. *Let n be odd positive number , then*

$$\left(\frac{-1}{n}\right) = \begin{cases} 1, & \text{if } n \equiv 1 \pmod 4 \\ -1, & \text{if } n \equiv 3 \pmod 4 \end{cases}$$

Lemma 2.3. *Let n be odd positive number , then*

$$\left(\frac{2}{n}\right) = \begin{cases} 1, & \text{if } n \equiv 1,7 \pmod 8 \\ -1, & \text{if } n \equiv 3,5 \pmod 8 \end{cases}$$

Lemma 2.4. *Let n be odd positive number , then case 1. ($n \equiv 1 \pmod 4$)*

$$\left(\frac{3}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod 3 \\ 0 & \text{if } n \equiv 0 \pmod 3 \\ -1 & \text{if } n \equiv 2 \pmod 3 \end{cases}$$

case 2. ($n \equiv 3 \pmod 4$)

$$\left(\frac{3}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 2 \pmod 3 \\ 0 & \text{if } n \equiv 0 \pmod 3 \\ -1 & \text{if } n \equiv 1 \pmod 3 \end{cases}$$

Proof. Since $3 \equiv 3 \pmod 4$ if we apply the law of quadratic reciprocity we have two cases . If $n \equiv 1 \pmod 4$ then $\left(\frac{3}{n}\right) = \left(\frac{n}{3}\right)$ and the result follows . If $n \equiv 3 \pmod 4$ then $\left(\frac{3}{n}\right) = -\left(\frac{n}{3}\right)$ and the result follows .

Lemma 2.5. *Let n be odd positive number , then*

$$\left(\frac{5}{n}\right) = \begin{cases} 1 & \textit{if } n \equiv 1,4 \pmod 5 \\ 0 & \textit{if } n \equiv 0 \pmod 5 \\ -1 & \textit{if } n \equiv 2,3 \pmod 5 \end{cases}$$

Proof. Since $5 \equiv 1 \pmod 4$ if we apply the law of quadratic reciprocity we have $\left(\frac{5}{n}\right) = \left(\frac{n}{5}\right)$ and the result follows .

Lemma 2.6. *Let n be odd positive number , then case 1. ($n \equiv 1 \pmod 4$)*

$$\left(\frac{-3}{n}\right) = \begin{cases} 1 & \textit{if } n \equiv 1,11 \pmod{12} \\ 0 & \textit{if } n \equiv 3,9 \pmod{12} \\ -1 & \textit{if } n \equiv 5,7 \pmod{12} \end{cases}$$

case 2. ($n \equiv 3 \pmod 4$)

$$\left(\frac{-3}{n}\right) = \begin{cases} 1 & \textit{if } n \equiv 5,7 \pmod{12} \\ 0 & \textit{if } n \equiv 3,9 \pmod{12} \\ -1 & \textit{if } n \equiv 1,11 \pmod{12} \end{cases}$$

Proof. $\left(\frac{-3}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{3}{n}\right)$. Applying the law of quadratic reciprocity we have : if $n \equiv 1 \pmod 4$ then $\left(\frac{3}{n}\right) = \left(\frac{n}{3}\right)$. If $n \equiv 3 \pmod 4$ then $\left(\frac{3}{n}\right) = -\left(\frac{n}{3}\right)$. Applying the Chinese remainder theorem in both cases several times we get the result .

Lemma 2.7. *Let n be odd positive number , then case 1. ($n \equiv 1 \pmod 4$)*

$$\left(\frac{7}{n}\right) = \begin{cases} 1 & \textit{if } n \equiv 1,2,4 \pmod 7 \\ 0 & \textit{if } n \equiv 0 \pmod 7 \\ -1 & \textit{if } n \equiv 3,5,6 \pmod 7 \end{cases}$$

case 2. ($n \equiv 3 \pmod 4$)

$$\left(\frac{7}{n}\right) = \begin{cases} 1 & \textit{if } n \equiv 3,5,6 \pmod 7 \\ 0 & \textit{if } n \equiv 0 \pmod 7 \\ -1 & \textit{if } n \equiv 1,2,4 \pmod 7 \end{cases}$$

Proof. Since $7 \equiv 3 \pmod 4$ if we apply the law of quadratic reciprocity we have two cases . If $n \equiv 1 \pmod 4$ then $\left(\frac{7}{n}\right) = \left(\frac{n}{7}\right)$ and the result follows . If $n \equiv 3 \pmod 4$ then $\left(\frac{7}{n}\right) = -\left(\frac{n}{7}\right)$ and the result follows .

Lemma 2.8. *Let n be odd positive number , then case 1. ($n \equiv 1 \pmod 4$)*

$$\left(\frac{-6}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1,5,19,23 \pmod{24} \\ 0 & \text{if } n \equiv 3,9,15,21 \pmod{24} \\ -1 & \text{if } n \equiv 7,11,13,17 \pmod{24} \end{cases}$$

case 2. ($n \equiv 3 \pmod 4$)

$$\left(\frac{-6}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 7,11,13,17 \pmod{24} \\ 0 & \text{if } n \equiv 3,9,15,21 \pmod{24} \\ -1 & \text{if } n \equiv 1,5,19,23 \pmod{24} \end{cases}$$

Proof. $\left(\frac{-6}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{2}{n}\right)\left(\frac{3}{n}\right)$. Applying the law of quadratic reciprocity we have : if $n \equiv 1 \pmod 4$ then $\left(\frac{3}{n}\right) = \left(\frac{n}{3}\right)$. If $n \equiv 3 \pmod 4$ then $\left(\frac{3}{n}\right) = -\left(\frac{n}{3}\right)$. Applying the Chinese remainder theorem in both cases several times we get the result .

Lemma 2.9. *Let n be odd positive number , then*

$$\left(\frac{10}{n}\right) = \begin{cases} 1 & \text{if } n \equiv 1,3,9,13,27,31,37,39 \pmod{40} \\ 0 & \text{if } n \equiv 5,15,25,35 \pmod{40} \\ -1 & \text{if } n \equiv 7,11,17,19,21,23,29,33 \pmod{40} \end{cases}$$

Proof. $\left(\frac{10}{n}\right) = \left(\frac{2}{n}\right)\left(\frac{5}{n}\right)$. Applying the law of quadratic reciprocity we have : $\left(\frac{5}{n}\right) = \left(\frac{n}{5}\right)$. Applying the Chinese remainder theorem several times we get the result .

The Main Result

Theorem 2.2. *Let $N = k \cdot 2^m - 1$ such that $m > 2$, $3 \mid k$, $0 < k < 2^m$ and*

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

Let $b = 3$ and $S_0(x) = V_k(b,1)$, thus
N is prime iff $N \mid S_{m-2}(x)$

Proof. Since $N \equiv 3 \pmod 4$ and $b = 3$ from Lemma 2.2 we know that $\left(\frac{2-b}{N}\right) = -1$. Similarly , since $N \equiv 2 \pmod 5$ or $N \equiv 3 \pmod 5$ and $b = 3$ from Lemma 2.5 we know that $\left(\frac{2+b}{N}\right) = -1$. From Lemma 2.1 we know that $V_k(b,1) = x$. Applying Theorem 2.1 in the case $c = 1$ we get the result.

Q.E.D.

Theorem 2.3. *Let $N = k \cdot 2^m - 1$ such that $m > 2$, $3 \mid k$, $0 < k < 2^m$ and*

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

Let $b = 5$ and $S_0(x) = V_k(b,1)$, thus N is prime iff $N \mid S_{m-2}(x)$

Proof. Since $N \equiv 3 \pmod{4}$ and $N \equiv 11 \pmod{12}$ and $b = 5$ from Lemma 2.6 we know that $\left(\frac{2-b}{N}\right) = -1$. Similarly , since $N \equiv 3 \pmod{4}$ and $N \equiv 1 \pmod{7}$ or $N \equiv 2 \pmod{7}$ or $N \equiv 4 \pmod{7}$ and $b = 5$ from Lemma 2.7 we know that $\left(\frac{2+b}{N}\right) = -1$. From Lemma 2.1 we know that $V_k(b,1) = x$. Applying Theorem 2.1 in the case $c = 1$ we get the result.

Q.E.D.

Theorem 2.4. *Let $N = k \cdot 2^m + 1$ such that $m > 2$, $0 < k < 2^m$ and*

$$\begin{cases} k \equiv 1 \pmod{42} \textit{ with } m \equiv 2,4 \pmod{6} \\ k \equiv 5 \pmod{42} \textit{ with } m \equiv 3 \pmod{6} \\ k \equiv 11 \pmod{42} \textit{ with } m \equiv 3,5 \pmod{6} \\ k \equiv 13 \pmod{42} \textit{ with } m \equiv 4 \pmod{6} \\ k \equiv 17 \pmod{42} \textit{ with } m \equiv 5 \pmod{6} \\ k \equiv 19 \pmod{42} \textit{ with } m \equiv 0 \pmod{6} \\ k \equiv 23 \pmod{42} \textit{ with } m \equiv 1,3 \pmod{6} \\ k \equiv 25 \pmod{42} \textit{ with } m \equiv 0,2 \pmod{6} \\ k \equiv 29 \pmod{42} \textit{ with } m \equiv 1,5 \pmod{6} \\ k \equiv 31 \pmod{42} \textit{ with } m \equiv 2 \pmod{6} \\ k \equiv 37 \pmod{42} \textit{ with } m \equiv 0,4 \pmod{6} \\ k \equiv 41 \pmod{42} \textit{ with } m \equiv 1 \pmod{6} \end{cases}$$

Let $b = 5$ and $S_0(x) = V_k(b,1)$, thus N is prime iff $N \mid S_{m-2}(x)$

Proof. Since $N \equiv 1 \pmod{4}$ and $N \equiv 5 \pmod{12}$ and $b = 5$ from Lemma 2.6 we know that $\left(\frac{2-b}{N}\right) = -1$. Similarly , since $N \equiv 1 \pmod{4}$ and $N \equiv 3 \pmod{7}$ or $N \equiv 5 \pmod{7}$ or $N \equiv 6 \pmod{7}$ and $b = 5$ from Lemma 2.7 we know that $\left(\frac{2+b}{N}\right) = -1$. From Lemma 2.1 we know that $V_k(b,1) = x$. Applying Theorem 2.1 in the case $c = 1$ we get the result.

Q.E.D.

Theorem 2.5. *Let $N = k \cdot 2^m + 1$ such that $m > 2$, $0 < k < 2^m$ and*

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

Let $b = 8$ and $S_0(x) = V_k(b, 1)$, thus N is prime iff $N \mid S_{m-2}(x)$

Proof. Since $N \equiv 1 \pmod 4$ and $N \equiv 17 \pmod{24}$ and $b = 8$ from Lemma 2.8 we know that $\left(\frac{2-b}{N}\right) = -1$. Similarly , since $N \equiv 17 \pmod{40}$ or $N \equiv 33 \pmod{40}$ and $b = 8$ from Lemma 2.9 we know that $\left(\frac{2+b}{N}\right) = -1$. From Lemma 2.1 we know that $V_k(b, 1) = x$. Applying Theorem 2.1 in the case $c = 1$ we get the result.

Q.E.D.

3 Three prime generating recurrences

Prime number generator I

Let $b_n = b_{n-1} + \mathrm{lcm}(\lfloor \sqrt{2} \cdot n \rfloor, b_{n-1})$ with $b_1 = 2$ then $a_n = b_{n+1}/b_n - 1$ is either 1 or prime .

Conjecture 3.1. *1. Every term of this sequence a_i is either prime or 1 .*
2. Every prime of the form $\lfloor \sqrt{2} \cdot n \rfloor$ is member of this sequence .

Prime number generator II

Let $b_n = b_{n-1} + \mathrm{lcm}(\lfloor \sqrt{3} \cdot n \rfloor, b_{n-1})$ with $b_1 = 3$ then $a_n = b_{n+1}/b_n - 1$ is either 1 or prime .

Conjecture 3.2. *1. Every term of this sequence a_i is either prime or 1 .*
2. Every prime of the form $\lfloor \sqrt{3} \cdot n \rfloor$ is member of this sequence .

Prime number generator III

Let $b_n = b_{n-1} + \mathrm{lcm}(\lfloor \sqrt{n^3} \rfloor, b_{n-1})$ with $b_1 = 2$ then $a_n = b_{n+1}/b_n - 1$ is either 1 or prime .

Conjecture 3.3. *1. Every term of this sequence a_i is either prime or 1 .*
2. Every prime of the form $\lfloor \sqrt{n^3} \rfloor$ is member of this sequence .

4 Some properties of Fibonacci numbers

Conjecture 4.1. *If p is prime , not 5 , and $M \geq 2$ then :*

$$M^{F_p} \equiv M^{(p-1)^{(1-\left(\frac{p}{5}\right))/2}} \pmod{\frac{M^p-1}{M-1}}$$

Conjecture 4.2. *If p is prime , and $M \geq 2$ then :*

$$M^{F_{p-\left(\frac{p}{5}\right)}} \equiv 1 \pmod{\frac{M^p-1}{M-1}}$$

Corollary of Cassini's formula

Corollary 4.1. *For $n \geq 2$:*

$$F_n = \begin{cases} \left\lfloor \sqrt{F_{n-1} \cdot F_{n+1}} \right\rfloor, & \text{if } n \text{ is even} \\ \left\lceil \sqrt{F_{n-1} \cdot F_{n+1}} \right\rceil, & \text{if } n \text{ is odd} \end{cases}$$

5 A modification of Riesel's primality test

Definition 5.1. 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 .

Corollary 5.1. *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 $n-2$.*
Let $S_i = P_{2^f}(S_{i-1})$ with $S_0 = P_k(4)$, thus
N is prime iff $S_{(n-2)/f} \equiv 0 \pmod{N}$

6 Primality criteria for specific classes of $N = k \cdot 2^n + 1$

Definition 6.1. 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 6.1. *Let $N = 3 \cdot 2^n + 1$ such that $n > 2$ and $n \equiv 1, 2 \pmod{4}$*
Let $S_i = P_2(S_{i-1})$ with

$$S_0 = \begin{cases} P_3(32), & \text{if } n \equiv 1 \pmod{4} \\ P_3(28), & \text{if } n \equiv 2 \pmod{4} \end{cases}$$

thus , N is prime iff $S_{n-2} \equiv 0 \pmod{N}$

Conjecture 6.2. *Let $N = 5 \cdot 2^n + 1$ such that $n > 2$ and $n \equiv 1, 3 \pmod{4}$*
Let $S_i = P_2(S_{i-1})$ with

$$S_0 = \begin{cases} P_5(28), & \text{if } n \equiv 1 \pmod{4} \\ P_5(32), & \text{if } n \equiv 3 \pmod{4} \end{cases}$$

thus , N is prime iff $S_{n-2} \equiv 0 \pmod{N}$

Conjecture 6.3. *Let $N = 7 \cdot 2^n + 1$ such that $n > 2$ and $n \equiv 0, 2 \pmod{4}$*
Let $S_i = P_2(S_{i-1})$ with

$$S_0 = \begin{cases} P_7(8), & \text{if } n \equiv 0 \pmod{4} \\ P_7(32), & \text{if } n \equiv 2 \pmod{4} \end{cases}$$

thus , N is prime iff $S_{n-2} \equiv 0 \pmod{N}$

Conjecture 6.4. *Let $N = 9 \cdot 2^n + 1$ such that $n > 3$ and $n \equiv 2, 3 \pmod{4}$*
Let $S_i = P_2(S_{i-1})$ with

$$S_0 = \begin{cases} P_9(28), & \textit{if } n \equiv 2 \pmod 4 \\ P_9(32), & \textit{if } n \equiv 3 \pmod 4 \end{cases}$$
thus, N is prime iff $S_{n-2} \equiv 0 \pmod N$

Conjecture 6.5. *Let $N = 11 \cdot 2^n + 1$ such that $n > 3$ and $n \equiv 1, 3 \pmod 4$*
Let $S_i = P_2(S_{i-1})$ with
$$S_0 = \begin{cases} P_{11}(8), & \textit{if } n \equiv 1 \pmod 4 \\ P_{11}(28), & \textit{if } n \equiv 3 \pmod 4 \end{cases}$$
thus , N is prime iff $S_{n-2} \equiv 0 \pmod N$

Conjecture 6.6. *Let $N = 13 \cdot 2^n + 1$ such that $n > 3$ and $n \equiv 0, 2 \pmod 4$*
Let $S_i = P_2(S_{i-1})$ with
$$S_0 = \begin{cases} P_{13}(32), & \textit{if } n \equiv 0 \pmod 4 \\ P_{13}(8), & \textit{if } n \equiv 2 \pmod 4 \end{cases}$$
thus , N is prime iff $S_{n-2} \equiv 0 \pmod N$

7 Congruence only holding for primes

Theorem 7.1. *(Wilson)*
A natural number $n > 1$ is a prime iff:

$$(n-1)! \equiv -1 \pmod n.$$

Theorem 7.2. *A natural number $n > 2$ is a prime iff:*

$$\prod_{k=1}^{n-1} k \equiv n-1 \pmod{\sum_{k=1}^{n-1} k}.$$

Proof
Necessity: If n is a prime, then

$$\prod_{k=1}^{n-1} k \equiv n-1 \pmod{\sum_{k=1}^{n-1} k}.$$

If n is an odd prime, then by Theorem 7.1 we have

$$\prod_{k=1}^{n-1} k \equiv n-1 \pmod n$$

Hence, $n \mid ((n-1)! - (n-1))$ and therefore $n \mid (n-1)((n-2)! - 1)$.
Since $n \not| (n-1)$ it follows $n \mid ((n-2)! - 1)$, hence

$$\frac{n(n-1)}{2} \mid (n-1)((n-2)! - 1),$$

thus

$$\prod_{k=1}^{n-1} k \equiv n-1 \pmod{\sum_{k=1}^{n-1} k}.$$

Sufficiency: If

$$\prod_{k=1}^{n-1} k \equiv n-1 \pmod{\sum_{k=1}^{n-1} k}$$

then n is a prime.

Suppose n is a composite and p is a prime such that $p \mid n$, then since $\sum_{k=1}^{n-1} k = \frac{n(n-1)}{2}$ it follows $p \mid \sum_{k=1}^{n-1} k$. Since

$$\prod_{k=1}^{n-1} k \equiv n-1 \pmod{\sum_{k=1}^{n-1} k},$$

we have

$$\prod_{k=1}^{n-1} k \equiv n-1 \pmod{p}.$$

However , since $p \leq n-1$ it divides $\prod_{k=1}^{n-1} k$, and so

$$\prod_{k=1}^{n-1} k \equiv 0 \pmod{p},$$

a contradiction . Hence n must be prime.

Q.E.D.

8 Primality test for $N = 2 \cdot 3^n - 1$

Definition 8.1. 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 8.1. *Let $N = 2 \cdot 3^n - 1$ such that $n > 1$.*
Let $S_i = P_3(S_{i-1})$ with $S_0 = P_3(a)$, where

$$a = \begin{cases} 6, & \textit{if } n \equiv 0 \pmod{2} \\ 8, & \textit{if } n \equiv 1 \pmod{2} \end{cases}$$

thus , N is prime iff $S_{n-1} \equiv a \pmod{N}$

9 Compositeness tests for specific classes of generalized Fermat numbers

Definition 9.1. 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 9.1. *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
If $F_n(b)$ is prime then $S_{2^n-2} \equiv 0 \pmod{F_n(b)}$

Conjecture 9.2. *Let $F_n(6) = 6^{2^n} + 1$ such that $n > 1$.*
Let $S_i = P_6(S_{i-1})$ with $S_0 = P_3(P_3(32))$, thus
If $F_n(6)$ is prime then $S_{2^n-2} \equiv 0 \pmod{F_n(6)}$

10 Primality tests for specific classes of $N = k \cdot 6^n - 1$

Definition 10.1. 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 10.1.

$$\textit{Let } N = k \cdot 6^n - 1 \textit{ such that } n > 2, k > 0,$$
$$k \equiv 2, 5 \pmod 7 \textit{ and } k < 6^n.$$
$$\textit{Let } S_i = P_6(S_{i-1}) \textit{ with } S_0 = P_{3k}(P_3(5)), \textit{ thus}$$
$$N \textit{ is prime iff } S_{n-2} \equiv 0 \pmod N$$

Conjecture 10.2.

$$\textit{Let } N = k \cdot 6^n - 1 \textit{ such that } n > 2, k > 0,$$
$$k \equiv 3, 4 \pmod 5 \textit{ and } k < 6^n.$$
$$\textit{Let } S_i = P_6(S_{i-1}) \textit{ with } S_0 = P_{3k}(P_3(3)), \textit{ thus}$$
$$N \textit{ is prime iff } S_{n-2} \equiv 0 \pmod N$$

Incomplete proof by mathlove

I'm going to prove that

$$\text{if } N \text{ is prime, then } S_{n-2} \equiv 0 \pmod N$$

for both conjectures.

(For the first conjecture)

First of all,

$$P_3(5) = 2^{-3} \cdot \left(\left(5 - \sqrt{21}\right)^3 + \left(5 + \sqrt{21}\right)^3 \right) = 110$$

So,

$$\begin{aligned}
S_0 = P_{3k}(P_3(5)) = P_{3k}(110) &= 2^{-3k} \cdot \left(\left(110 - \sqrt{110^2 - 4}\right)^{3k} + \left(110 + \sqrt{110^2 - 4}\right)^{3k} \right) \\
&= \left(\frac{110 - \sqrt{110^2 - 4}}{2} \right)^{3k} + \left(\frac{110 + \sqrt{110^2 - 4}}{2} \right)^{3k} \\
&= \left(55 - 12\sqrt{21}\right)^{3k} + \left(55 + 12\sqrt{21}\right)^{3k} \\
&= (a^2)^{3k} + (b^2)^{3k} \\
&= a^{6k} + b^{6k}
\end{aligned}$$

where $a = 2\sqrt{7} - 3\sqrt{3}, b = 2\sqrt{7} + 3\sqrt{3}$ with $ab = 1$.

From this, we can prove by induction that

$$S_i = a^{6^{i+1}k} + b^{6^{i+1}k}.$$

Thus,

$$\begin{aligned}
S_{n-2} = a^{\frac{N+1}{6}} + b^{\frac{N+1}{6}} = \left(\frac{\sqrt{7}}{2} - \frac{\sqrt{3}}{2} \right)^{\frac{N+1}{2}} + \left(\frac{\sqrt{7}}{2} + \frac{\sqrt{3}}{2} \right)^{\frac{N+1}{2}} = \\
= 2^{-\frac{N+1}{2}} \left((\sqrt{7} - \sqrt{3})^{\frac{N+1}{2}} + (\sqrt{7} + \sqrt{3})^{\frac{N+1}{2}} \right).
\end{aligned}$$

By the way, for N prime,

$$\begin{aligned}
(\sqrt{7} - \sqrt{3})^{N+1} + (\sqrt{7} + \sqrt{3})^{N+1} &= \sum_{i=0}^{N+1} \binom{N+1}{i} \left(\sqrt{7}\right)^i ((-\sqrt{3})^{N+1-i} + (\sqrt{3})^{N+1-i}) \\
&= \sum_{j=0}^{(N+1)/2} \binom{N+1}{2j} \left(\sqrt{7}\right)^{2j} \cdot 2(\sqrt{3})^{N+1-2j} \\
&= \sum_{j=0}^{(N+1)/2} \binom{N+1}{2j} 7^j \cdot 2 \cdot 3^{\frac{N+1}{2} - j} \\
&\equiv 2 \cdot 3^{\frac{N+1}{2}} + 7^{\frac{N+1}{2}} \cdot 2 \pmod{N} \\
&\equiv 2 \cdot 3 + (-7) \cdot 2 \pmod{N} \\
&\equiv -8 \pmod{N}
\end{aligned}$$

This is because $N \equiv 2 \pmod 3$ and $N \equiv \pm 2 \cdot (-1)^n - 1 \equiv 1, 4 \pmod 7$ implies that

$$3^{(N-1)/2} \equiv 1 \pmod{N}, \quad 7^{(N-1)/2} \equiv -1 \pmod{N}.$$

From this, since $2^{N-1} \equiv 1 \pmod N$,

$$\begin{aligned}
2^{N+1} S_{n-2}^2 &= (\sqrt{7} - \sqrt{3})^{N+1} + (\sqrt{7} + \sqrt{3})^{N+1} + 2 \cdot 4^{\frac{N+1}{2}} \\
&\equiv -8 + 2 \cdot 2^{N-1} \cdot 4 \pmod{N} \\
&\equiv 0 \pmod{N}
\end{aligned}$$

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

Q.E.D.

(For the second conjecture)

$$P_3(3) = 2^{-3} \cdot \left(\left(3 - \sqrt{5}\right)^3 + \left(3 + \sqrt{5}\right)^3 \right) = 18$$

$$\begin{aligned} S_0 = P_{3k}(P_3(3)) &= 2^{-3k} \cdot \left(\left(18 - \sqrt{18^2 - 4}\right)^{3k} + \left(18 + \sqrt{18^2 - 4}\right)^{3k} \right) \\ &= (9 - 4\sqrt{5})^{3k} + (9 + 4\sqrt{5})^{3k} = c^{6k} + d^{6k} \end{aligned}$$

where $c = \sqrt{5} - 2, d = \sqrt{5} + 2$ with $cd = 1$.

We can prove by induction that

$$S_i = c^{6^{i+1}k} + d^{6^{i+1}k}$$

Thus,

$$\begin{aligned} S_{n-2} = c^{\frac{N+1}{6}} + d^{\frac{N+1}{6}} &= \left(\frac{\sqrt{5}}{2} - \frac{1}{2} \right)^{\frac{N+1}{2}} + \left(\frac{\sqrt{5}}{2} + \frac{1}{2} \right)^{\frac{N+1}{2}} = \\ &= 2^{-\frac{N+1}{2}} \left(\left(\sqrt{5} - 1\right)^{\frac{N+1}{2}} + \left(\sqrt{5} + 1\right)^{\frac{N+1}{2}} \right). \end{aligned}$$

By the way, for N prime,

$$\begin{aligned} \left(\sqrt{5} - 1\right)^{N+1} + \left(\sqrt{5} + 1\right)^{N+1} &= \sum_{i=0}^{N+1} \binom{N+1}{i} (\sqrt{5})^i \left((-1)^{N+1-i} + 1^{N+1-i}\right) \\ &= \sum_{j=0}^{(N+1)/2} \binom{N+1}{2j} (\sqrt{5})^{2j} \cdot 2 \\ &= \sum_{j=0}^{(N+1)/2} \binom{N+1}{2j} 5^j \cdot 2 \\ &\equiv 2 + 5^{\frac{N+1}{2}} \cdot 2 \pmod{N} \\ &\equiv 2 + (-5) \cdot 2 \pmod{N} \\ &\equiv -8 \pmod{N} \end{aligned}$$

This is because $N \equiv 2, 3 \pmod{5}$ implies that

$$5^{\frac{N-1}{2}} \equiv -1 \pmod{N}.$$

From this, since $2^{N-1} \equiv 1 \pmod{N}$,

$$\begin{aligned} 2^{N+1} S_{n-2}^2 &= (\sqrt{5} - 1)^{N+1} + (\sqrt{5} + 1)^{N+1} + 2 \cdot 4^{\frac{N+1}{2}} \\ &\equiv -8 + 2 \cdot 2^{N-1} \cdot 4 \pmod{N} \\ &\equiv 0 \pmod{N} \end{aligned}$$

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

Q.E.D.

11 Compositeness tests for specific classes of $N = k \cdot b^n - 1$

Definition 11.1. 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 11.1. *Let* $N = k \cdot b^n - 1$ *such that* $n > 2$ *,* k *is odd ,* $3 \nmid k$ *,* b *is even ,* $3 \nmid b$ *,* $k < b^n$ *.*
Let $S_i = P_b(S_{i-1})$ *with* $S_0 = P_{bk/2}(P_{b/2}(4))$ *, thus*
if N *is prime then* $S_{n-2} \equiv 0 \pmod{N}$

Conjecture 11.2. *Let* $N = k \cdot b^n - 1$ *such that* $n > 2$ *,* $k < b^n$ *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* $S_0 = P_{bk/2}(P_{b/2}(18))$ *, thus*
If N *is prime then* $S_{n-2} \equiv 0 \pmod{N}$

Conjecture 11.3. *Let* $N = k \cdot b^n - 1$ *such that* $n > 2$ *,* $k < b^n$ *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* $S_0 = P_{bk/2}(P_{b/2}(18))$ *, thus*
If N *is prime then* $S_{n-2} \equiv 0 \pmod{N}$

Conjecture 11.4. *Let* $N = k \cdot b^n - 1$ *such that* $n > 2$ *,* $k < b^n$ *and*
$$\begin{cases} k \equiv 21 \pmod{30} \text{ with } b \equiv 2 \pmod{10} \text{ and } n \equiv 2,3 \pmod{4} \\ k \equiv 21 \pmod{30} \text{ with } b \equiv 4 \pmod{10} \text{ and } n \equiv 1,3 \pmod{4} \\ k \equiv 21 \pmod{30} \text{ with } b \equiv 8 \pmod{10} \text{ and } n \equiv 1,2 \pmod{4} \end{cases}$$
Let $S_i = P_b(S_{i-1})$ *with* $S_0 = P_{bk/2}(P_{b/2}(3))$ *, thus*
If N *is prime then* $S_{n-2} \equiv 0 \pmod{N}$

12 Compositeness tests for specific classes of $N = k \cdot 3^n \pm 2$

Definition 12.1. 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 12.1. *Let* $N = k \cdot 3^n - 2$ *such that* $n \equiv 0 \pmod{2}$ *,* $n > 2$ *,* $k \equiv 1 \pmod{4}$ *and* $k > 0$ *.*
Let $S_i = P_3(S_{i-1})$ *with* $S_0 = P_{3k}(4)$ *, thus*
If N *is prime then* $S_{n-1} \equiv P_1(4) \pmod{N}$

Conjecture 12.2. *Let* $N = k \cdot 3^n - 2$ *such that* $n \equiv 1 \pmod 2$, $n > 2$, $k \equiv 1 \pmod 4$ *and* $k > 0$.
Let $S_i = P_3(S_{i-1})$ *with* $S_0 = P_{3k}(4)$ *, thus*
If N *is prime then* $S_{n-1} \equiv P_3(4) \pmod N$

Conjecture 12.3. *Let* $N = k \cdot 3^n + 2$ *such that* $n > 2$, $k \equiv 1, 3 \pmod 8$ *and* $k > 0$.
Let $S_i = P_3(S_{i-1})$ *with* $S_0 = P_{3k}(6)$ *, thus*
If N *is prime then* $S_{n-1} \equiv P_3(6) \pmod N$

Conjecture 12.4. *Let* $N = k \cdot 3^n + 2$ *such that* $n > 2$, $k \equiv 5, 7 \pmod 8$ *and* $k > 0$.
Let $S_i = P_3(S_{i-1})$ *with* $S_0 = P_{3k}(6)$ *, thus*
If N *is prime then* $S_{n-1} \equiv P_1(6) \pmod N$

13 Compositeness tests for $N = b^n \pm b \pm 1$

Definition 13.1. 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 13.1. *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 13.2. *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 13.3. *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 13.4. *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* $S_{n-1} \equiv -P_{(b+2)/2}(6) \pmod N$.

Conjecture 13.5. *Let* $N = b^n - b + 1$ *such that* $n > 3$, $b \equiv 0, 2 \pmod 8$.
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 13.6. *Let* $N = b^n - b + 1$ *such that* $n > 3$, $b \equiv 4, 6 \pmod 8$.
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 13.7. *Let* $N = b^n + b - 1$ *such that* $n > 3$, $b \equiv 0, 2 \pmod{8}$.
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 13.8. *Let* $N = b^n + b - 1$ *such that* $n > 3$, $b \equiv 4, 6 \pmod{8}$.
Let $S_i = P_b(S_{i-1})$ *with* $S_0 = P_{b/2}(6)$,
thus
if N *is prime, then* $S_{n-1} \equiv -P_{b/2}(6) \pmod{N}$.

Proof attempt by mathlove

First of all,

$$\begin{aligned} S_0 = P_{b/2}(6) &= 2^{-\frac{b}{2}} \cdot \left(\left(6 - 4\sqrt{2}\right)^{\frac{b}{2}} + \left(6 + 4\sqrt{2}\right)^{\frac{b}{2}} \right) \\ &= \left(3 - 2\sqrt{2}\right)^{\frac{b}{2}} + \left(3 + 2\sqrt{2}\right)^{\frac{b}{2}} \\ &= \left(\sqrt{2} - 1\right)^{b} + \left(\sqrt{2} + 1\right)^{b} \\ &= p^b + q^b \end{aligned}$$

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

Now, we can prove by induction that

$$S_i = p^{b^{i+1}} + q^{b^{i+1}}.$$

By the way,

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

Also,

$$\begin{aligned} p^{N+3} + q^{N+3} &= \sum_{i=0}^{N+3} \binom{N+3}{i} (\sqrt{2})^i \left((-1)^{N+3-i} + 1\right) \\ &= \sum_{j=0}^{(N+3)/2} \binom{N+3}{2j} 2^{j+1} \\ &\equiv 2 + \binom{N+3}{2} \cdot 2^2 + \binom{N+3}{N+1} \cdot 2^{\frac{N+3}{2}} + 2^{\frac{N+5}{2}} \pmod{N} \\ &\equiv 14 + 12 \cdot 2^{\frac{N-1}{2}} + 8 \cdot 2^{\frac{N-1}{2}} \pmod{N} \end{aligned} \tag{2}$$

Here, for $N \equiv \pm 1 \pmod 8$, since $2^{\frac{N-1}{2}} \equiv 1 \pmod N$, from $(1)(2)$, we can prove by induction that

$$p^{N+2i-1} + q^{N+2i-1} \equiv p^{2i} + q^{2i} \pmod N \qquad (3)$$

For $N \equiv 3, 5 \pmod 8$, since $2^{\frac{N-1}{2}} \equiv -1 \pmod N$, from $(1)(2)$, we can prove by induction that

$$p^{N+2i-1} + q^{N+2i-1} \equiv -\left(p^{2i-2} + q^{2i-2}\right) \pmod N \qquad (4)$$

To prove $(3)(4)$, we can use

$$p^{N+2(i+1)-1} + q^{N+2(i+1)-1} \equiv \left(p^{N+2i-1} + q^{N+2i-1}\right)\left(p^2 + q^2\right) -$$
$$- \left(p^{N+2(i-1)-1} + q^{N+2(i-1)-1}\right) \pmod N$$

and

$$p^{N+2(i-1)-1} + q^{N+2(i-1)-1} \equiv \left(p^{N+2i-1} + q^{N+2i-1}\right)\left(p^{-2} + q^{-2}\right) -$$
$$- \left(p^{N+2(i+1)-1} + q^{N+2(i+1)-1}\right) \pmod N$$

(Note that $(3)(4)$ holds for **every integer** i (not necessarily positive) because of $pq = 1$.)

Conjecture 13.1 is true because from (3)

$$\begin{aligned} S_{n-1} &= p^{N+b+1} + q^{N+b+1} \\ &\equiv p^{b+2} + q^{b+2} \pmod N \\ &\equiv P_{(b+2)/2}(6) \pmod N \end{aligned}$$

Conjecture 13.2 is true because from (4)

$$\begin{aligned} S_{n-1} &= p^{N+b+1} + q^{N+b+1} \\ &\equiv -\left(p^{b} + q^{b}\right) \pmod N \\ &\equiv -P_{b/2}(6) \pmod N \end{aligned}$$

Conjecture 13.3 is true because from (3)

$$\begin{aligned} S_{n-1} &= p^{N-b-1} + q^{N-b-1} \\ &\equiv p^{-b} + q^{-b} \pmod N \\ &\equiv q^{b} + p^{b} \pmod N \\ &\equiv P_{b/2}(6) \pmod N \end{aligned}$$

Conjecture 13.4 is true because from (4)

$$\begin{aligned} S_{n-1} &= p^{N-b-1} + q^{N-b-1} \\ &\equiv -\left(p^{-b-2} + q^{-b-2}\right) \pmod N \\ &\equiv -\left(q^{b+2} + p^{b+2}\right) \pmod N \\ &\equiv -P_{(b+2)/2}(6) \pmod N \end{aligned}$$

Conjecture 13.5 is true because from (3)

$$\begin{aligned} S_{n-1} &= p^{N+b-1} + q^{N+b-1} \\ &\equiv p^b + q^b \pmod{N} \\ &\equiv P_{b/2}(6) \pmod{N} \end{aligned}$$

Conjecture 13.6 is true because from (4)

$$\begin{aligned} S_{n-1} &= p^{N+b-1} + q^{N+b-1} \\ &\equiv -\left(p^{b-2} + q^{b-2}\right) \pmod{N} \\ &\equiv -P_{(b-2)/2}(6) \pmod{N} \end{aligned}$$

Conjecture 13.7 is true because from (3)

$$\begin{aligned} S_{n-1} &= p^{N-b+1} + q^{N-b+1} \\ &\equiv p^{-b+2} + q^{-b+2} \pmod{N} \\ &\equiv q^{b-2} + p^{b-2} \pmod{N} \\ &\equiv P_{(b-2)/2}(6) \pmod{N} \end{aligned}$$

Conjecture 13.8 is true because from (4)

$$\begin{aligned} S_{n-1} &= p^{N-b+1} + q^{N-b+1} \\ &\equiv -\left(p^{-b} + q^{-b}\right) \pmod{N} \\ &\equiv -\left(q^{b} + p^{b}\right) \pmod{N} \\ &\equiv -P_{b/2}(6) \pmod{N} \end{aligned}$$

Q.E.D.

14 Primality test for $N = 8 \cdot 3^n - 1$

Definition 14.1. 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 14.1. *Let* $N = 8 \cdot 3^n - 1$ *such that* $n > 1$.
Let $S_i = P_3(S_{i-1})$ *with* $S_0 = P_{12}(4)$
thus ,
N *is prime iff* $S_{n-1} \equiv 4 \pmod{N}$

Incomplete proof by David Speyer
Let's unwind your formula.

$$S_{n-1} = P_{4 \cdot 3^n}(4) = (2+\sqrt{3})^{4 \cdot 3^n} + (2-\sqrt{3})^{4 \cdot 3^n}$$

$$= (2+\sqrt{3})^{4 \cdot 3^n} + (2+\sqrt{3})^{-4 \cdot 3^n} = (2+\sqrt{3})^{(N+1)/2} + (2+\sqrt{3})^{-(N+1)/2}.$$

You are testing whether or not $S_{n-1} \equiv 4 \bmod N$ or, on other words,

$$(2+\sqrt{3})^{(N+1)/2} + (2+\sqrt{3})^{-(N+1)/2} \equiv 4 \bmod N. \quad (*)$$

If N is prime: (This section is rewritten to use some observations about roots of unity. It may therefore look a bit less motivated.) The prime N is $-1 \bmod 24$, so $N^2 \equiv 1 \bmod 24$ and the finite field $\mathbb{F}_{N^2}$ contains a primitive 24-th root of unity, call it η. We have $(\eta+\eta^{-1})^2 = 2+\sqrt{3}$, for one of the two choices of $\sqrt{3}$ in $\mathbb{F}_N$. (Since $N \equiv -1 \bmod 12$, we have $\left(\frac{3}{N}\right) = 1$.) Now, $\eta \notin \mathbb{F}_N$. However, we compute $(\eta+\eta^{-1})^N = \eta^N + \eta^{-N} = \eta^{-1} + \eta$, since $N \equiv -1 \bmod 24$. So $\eta + \eta^{-1} \in \mathbb{F}_N$ and we deduce that $2+\sqrt{3}$ is a square in $\mathbb{F}_N$.

So $(2+\sqrt{3})^{(N-1)/2} \equiv 1 \bmod N$ and $(2+\sqrt{3})^{(N+1)/2} \equiv (2+\sqrt{3}) \bmod N$. Similarly, $(2+\sqrt{3})^{-(N+1)/2} \equiv (2+\sqrt{3})^{-1} \equiv 2-\sqrt{3} \bmod N$ and $(*)$ holds.

If N is not prime. Earlier, I said that I saw no way to control whether or not $(*)$ held when N was composite. I said that there seemed to be no reason it should hold and that, furthermore, it was surely very rare, because N is exponentially large, so it is unlikely for a random equality to hold modulo N.

Since then I had a few more ideas about the problem, which don't make it seem any easier, but clarify to me why it is so hard. To make life easier, let's assume that $N = p_1 p_2 \cdots p_j$ is square free. Of course, $(*)$ holds modulo N if and only if it holds modulo every p_i.

Let η be a primitive 24-th root of unity in an appropriate extension of $\mathbb{F}_{p_j}$. The following equations all take place in this extension of $\mathbb{F}_{p_j}$. It turns out that $(*)$ factors quite a bit:

$$(2+\sqrt{3})^{(N+1)/2} + (2+\sqrt{3})^{-(N+1)/2} = 4$$

$$(2+\sqrt{3})^{(N+1)/2} = 2 \pm \sqrt{3}$$

$$(\eta+\eta^{-1})^{(N+1)} = (\eta+\eta^{-1})^2 \text{ or } (\eta^5+\eta^{-5})^2$$

$$(\eta+\eta^{-1})^{(N+1)/2} \in \{\eta+\eta^{-1},\ \eta^3+\eta^{-3},\ \eta^5+\eta^{-5}, \eta^7+\eta^{-7}\}. \quad (\dagger)$$

Here is what I would like to do at this point, to follow the lines of the Lucas-Lehmer test, but cannot.

(1) I'd like to know that $(\eta+\eta^{-1})^{(N+1)/2} = \eta+\eta^{-1}$, not one of the other options in $(\dagger)$. (This is what actually occurs in the N prime case, as shown previously.) This would imply that $(\eta+\eta^{-1})^{(N-1)/2} = 1 \in \mathbb{F}_{p_j}$.

(2) I'd like to know that the order of $\eta+\eta^{-1}$ was precisely $(N-1)/2$, not some divisor thereof.

(3) I'd like to thereby conclude that the multiplicative group of $\mathbb{F}_{p_j}$ was of order divisible by $(N-1)/2$, and thus $p_j \geq (N-1)/2$. This would mean that there was basically only room for one p_j, and we would be able to conclude primality.

Now, (1) isn't so bad, because you could directly compute in the ring $\mathbb{Z}/(N\mathbb{Z})[\eta]/(\eta^8-\eta^4+1)$, rather than trying to disguise this ring with elementary polynomial formulas. So, while I don't see that your algorithm checks this point, it wouldn't be hard.

And $(2) \implies (3)$ is correct.

But you have a real problem with (2). This way this works in the Lucas-Lehmer test is that you are trying to prove that $2+\sqrt{3}$ has order precisely 2^p in the field $\mathbb{F}_{2^p-1}[\sqrt{3}] \cong \mathbb{F}_{(2^p-1)^2}$. You already know that $(2+\sqrt{3})^{2^p}=1$. So it is enough to check that $(2+\sqrt{3})^{2^{p-1}}=-1$, not 1.

In the current situation, the analogous thing would be to check that $(\eta+\eta^{-1})^{(N-1)/(2q)} \neq 1$ for every prime q dividing $(N-1)/2$. But I have no idea which primes divide q! This seems like an huge obstacle to a proof that $(*)$ implies N is prime.

To repeat: I think it may well be true that $(*)$ implies N is prime, simply because there is no reason that $(\dagger)$ should hold once $N \neq p_j$, and the odds of $(\dagger)$ happening by accident are exponentially small. But I see no global principle implying this.

Q.E.D.

15 Generalization of Kilford's primality theorem

Conjecture 15.1. *Natural number n greater than two is prime iff :*

$$\prod_{k=1}^{n-1}\left(b^k-a\right) \equiv \frac{a^n-1}{a-1} \pmod{\frac{b^n-1}{b-1}}$$

where $b>a>1$.

16 Prime generating sequence

Definition 16.1. Let $b_n=b_{n-2}+\operatorname{lcm}(n-1,b_{n-2})$ with $b_1=2$, $b_2=2$ and $n>2$.
Let $a_n=b_{n+2}/b_n-1$

Conjecture 16.1. *1. Every term of this sequence a_i is either prime or* 1 *.*
2. Every odd prime number is member of this sequence .
3. Every new prime in sequence is a next prime from the largest prime already listed .

Incomplete proof by Markus Schepherd

This is the full argument for conjectures 2 and 3. First we need the general relation between gcd (a,b) and lcm $[a,b]$: $a\cdot b=(a,b)\cdot[a,b]$. Then we note that the lowest common multiple $[n-1,b_{n-2}]$ is in particular a multiple of b_{n-2}, say kb_{n-2} with $1\leq k\leq n-1$. Hence we have $b_n=b_{n-2}(k+1)$, so in every step the term b_n gets a new factor between 2 and n which means in particular that all prime factors of b_n are less or equal to n. Now we rearrange a_n with the above observation to $a_n=\frac{n+1}{(n+1,b_n)}$. Let p be a prime. Then $(p,b_{p-1})=1$ since all prime factors of b_{p-1} are strictly smaller than p. But then $a_{p-1}=\frac{p}{(p,b_{p-1})}=p$ as claimed in conjecture 2. Further, we have obviously $a_n\leq n+1$ for all n, so the first index for which the prime p can appear in the sequence is $p-1$ which immediately implies conjecture 3.

Q.E.D.

17 Primality test using Euler's totient function

Theorem 17.1. *(Wilson)*
A positive integer n is prime iff $(n-1)! \equiv -1 \pmod{n}$

Theorem 17.2. *A positive integer n is prime iff $\varphi(n)! \equiv -1 \pmod{n}$.*

Proof
Necessity : *If n is prime then $\varphi(n)! \equiv -1 \pmod{n}$*
If n is prime then we have $\varphi(n) = n-1$ and
by Theorem 17.1 : $(n-1)! = -1 \pmod{n}$,
hence $\varphi(n)! \equiv -1 \pmod{n}$.
Sufficiency : *If $\varphi(n)! \equiv -1 \pmod{n}$ then n is prime*
For $n = 2$ and $n = 6$:
$\varphi(2)! \equiv -1 \pmod{2}$ and 2 is prime .
$\varphi(6)! \not\equiv -1 \pmod{6}$ and 6 is composite .
For $n \neq 2, 6$:
Suppose n is composite and p is the least prime such that $p \mid n$,
then we have $\varphi(n)! \equiv -1 \pmod{p}$.
Since $\varphi(n) \geq \sqrt{n}$ for all n except $n = 2$ and $n = 6$
and $p \leq \sqrt{n}$ it follows $p \mid \varphi(n)!$, hence $\varphi(n)! \equiv 0 \pmod{p}$
a contradiction .
Therefore , n must be prime .
Q.E.D.

18 Primality tests for specific classes of Proth numbers

Theorem 18.1. *Let $N = k \cdot 2^n + 1$ with $n > 1$, $k < 2^n$, $3 \mid k$, and*

$$\begin{cases} k \equiv 3 \pmod{30}, & \textit{with } n \equiv 1, 2 \pmod{4} \\ k \equiv 9 \pmod{30}, & \textit{with } n \equiv 2, 3 \pmod{4} \\ k \equiv 21 \pmod{30}, & \textit{with } n \equiv 0, 1 \pmod{4} \\ k \equiv 27 \pmod{30}, & \textit{with } n \equiv 0, 3 \pmod{4} \end{cases}$$

thus,
N is prime iff $5^{\frac{N-1}{2}} \equiv -1 \pmod{N}$.

Proof
Necessity : *If N is prime then $5^{\frac{N-1}{2}} \equiv -1 \pmod{N}$*
Let N be a prime , then by Euler criterion :
$5^{\frac{N-1}{2}} \equiv \left(\frac{5}{N}\right) \pmod{N}$
If N is a prime then $N \equiv 2, 3 \pmod{5}$ and therefore : $\left(\frac{N}{5}\right) = -1$.
Since $N \equiv 1 \pmod{4}$ according to the law of quadratic reciprocity it follows that : $\left(\frac{5}{N}\right) = -1$.
Hence , $5^{\frac{N-1}{2}} \equiv -1 \pmod{N}$.

Sufficiency : *If* $5^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ *then* N *is prime*

If $5^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ then by Proth's theorem N is prime .

Q.E.D.

Theorem 18.2. *Let* $N = k \cdot 2^n + 1$ *with* $n > 1$, $k < 2^n$, $3 \mid k$, *and*

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

thus , N *is prime iff* $7^{\frac{N-1}{2}} \equiv -1 \pmod{N}$

Proof

Necessity : *If* N *is prime then* $7^{\frac{N-1}{2}} \equiv -1 \pmod{N}$

Let N be a prime , then by Euler criterion :

$7^{\frac{N-1}{2}} \equiv \left(\frac{7}{N}\right) \pmod{N}$

If N is prime then $N \equiv 3,5,6 \pmod{7}$ and therefore : $\left(\frac{N}{7}\right) = -1$.

Since $N \equiv 1 \pmod{4}$ according to the law of quadratic reciprocity it follows that : $\left(\frac{7}{N}\right) = -1$.

Hence , $7^{\frac{N-1}{2}} \equiv -1 \pmod{N}$.

Sufficiency : *If* $7^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ *then* N *is prime*

If $7^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ then by Proth's theorem N is prime .

Q.E.D.

Theorem 18.3. *Let* $N = k \cdot 2^n + 1$ *with* $n > 1$, $k < 2^n$, $3 \mid k$, *and*

$$\begin{cases} k \equiv 3 \pmod{66}, & \textit{with } n \equiv 1,2,6,8,9 \pmod{10} \\ k \equiv 9 \pmod{66}, & \textit{with } n \equiv 0,1,3,4,8 \pmod{10} \\ k \equiv 15 \pmod{66}, & \textit{with } n \equiv 2,4,5,7,8 \pmod{10} \\ k \equiv 21 \pmod{66}, & \textit{with } n \equiv 1,2,4,5,9 \pmod{10} \\ k \equiv 27 \pmod{66}, & \textit{with } n \equiv 0,2,3,5,6 \pmod{10} \\ k \equiv 39 \pmod{66}, & \textit{with } n \equiv 0,1,5,7,8 \pmod{10} \\ k \equiv 45 \pmod{66}, & \textit{with } n \equiv 0,4,6,7,9 \pmod{10} \\ k \equiv 51 \pmod{66}, & \textit{with } n \equiv 0,2,3,7,9 \pmod{10} \\ k \equiv 57 \pmod{66}, & \textit{with } n \equiv 3,5,6,8,9 \pmod{10} \\ k \equiv 63 \pmod{66}, & \textit{with } n \equiv 1,3,4,6,7 \pmod{10} \end{cases}$$

thus,

N *is prime iff* $11^{\frac{N-1}{2}} \equiv -1 \pmod{N}$

Proof

Necessity : *If N is prime then* $11^{\frac{N-1}{2}} \equiv -1 \pmod{N}$

Let N be a prime , then by Euler criterion :
$11^{\frac{N-1}{2}} \equiv \left(\frac{11}{N}\right) \pmod{N}$
If N is prime then $N \equiv 2,6,7,8,10 \pmod{11}$ and therefore : $\left(\frac{N}{11}\right) = -1$.
Since $N \equiv 1 \pmod{4}$ according to the law of quadratic reciprocity it follows that : $\left(\frac{11}{N}\right) = -1$.
Hence , $11^{\frac{N-1}{2}} \equiv -1 \pmod{N}$.

Sufficiency : *If* $11^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ *then N is prime*

If $11^{\frac{N-1}{2}} \equiv -1 \pmod{N}$ then by Proth's theorem N is prime .

Q.E.D.

19 Generalization of Wilson's primality theorem

Theorem 19.1. *For $m \geq 1$ number n greater than one is prime iff :*

$$(n^m - 1)! \equiv (n-1)^{\left\lceil \frac{(-1)^{m+1}}{2} \right\rceil} \cdot n^{\frac{n^m - mn + m - 1}{n-1}} \pmod{n^{\frac{n^m - mn + m + n - 2}{n-1}}}$$

20 Primality test for Fermat numbers using quartic recurrence equation

Let us define sequence S_i as :

$$S_i = \begin{cases} 8 & \text{if } i = 0; \\ (S_{i-1}^2 - 2)^2 - 2 & \text{otherwise .} \end{cases}$$

Theorem 20.1. $F_n = 2^{2^n} + 1, (n \geq 2)$ *is a prime if and only if F_n divides* $S_{2^{n-1}-1}$.

Proof

Let us define $\omega = 4 + \sqrt{15}$ and $\bar{\omega} = 4 - \sqrt{15}$ and then define L_n to be $\omega^{2^{2n}} + \bar{\omega}^{2^{2n}}$, we get $L_0 = \omega + \bar{\omega} = 8$, and $L_{n+1} = \omega^{2^{2n+2}} + \bar{\omega}^{2^{2n+2}} = (\omega^{2^{2n+1}})^2 + (\bar{\omega}^{2^{2n+1}})^2 == (\omega^{2^{2n+1}} + \bar{\omega}^{2^{2n+1}})^2 - 2 \cdot \omega^{2^{2n+1}} \cdot \bar{\omega}^{2^{2n+1}} == ((\omega^{2^{2n}} + \bar{\omega}^{2^{2n}})^2 - 2 \cdot \omega^{2^{2n}} \cdot \bar{\omega}^{2^{2n}})^2 - 2 \cdot \omega^{2^{2n+1}} \cdot \bar{\omega}^{2^{2n+1}} = = ((\omega^{2^{2n}} + \bar{\omega}^{2^{2n}})^2 - 2 \cdot (\omega \cdot \bar{\omega})^{2^{2n}})^2 - 2 \cdot (\omega \cdot \bar{\omega})^{2^{2n+1}}$ and since $\omega \cdot \bar{\omega} = 1$ we get : $L_{n+1} = (L_n^2 - 2)^2 - 2$
Because the L_n satisfy the same inductive definition as the sequence S_i , the two sequences must be the same .

Proof of necessity

If $2^{2^n} + 1$ is prime then $S_{2^{n-1}-1}$ is divisible by $2^{2^n} + 1$

We rely on simplification of the proof of Lucas-Lehmer test by Oystein J. R. Odseth .First notice that 3 is quadratic non-residue $\pmod{F_n}$ and that 5 is quadratic non-residue $\pmod{F_n}$. Euler's criterion then gives us : $3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$ and $5^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$ On the other hand 2 is a quadratic-residue $\pmod{F_n}$, Euler's criterion gives: $2^{\frac{F_n-1}{2}} \equiv 1 \pmod{F_n}$

Next define $\sigma = 2\sqrt{15}$, and define X as the multiplicative group of $\{a + b\sqrt{15} | a, b \in Z_{F_n}\}$ .We will use following lemmas :

Lemma 1. $(x+y)^{F_n} = x^{F_n} + y^{F_n} \pmod{F_n}$
Lemma 2. $a^{F_n} \equiv a \pmod{F_n}$ (Fermat little theorem)

Then in group X we have :

$(6+\sigma)^{F_n} \equiv (6)^{F_n} + (\sigma)^{F_n} \pmod{F_n} == 6 + (2\sqrt{15})^{F_n} \pmod{F_n} == 6 + 2^{F_n} \cdot 15^{\frac{F_n-1}{2}} \cdot \sqrt{15} \pmod{F_n} == 6 + 2 \cdot 3^{\frac{F_n-1}{2}} \cdot 5^{\frac{F_n-1}{2}} \cdot \sqrt{15} \pmod{F_n} == 6 + 2 \cdot (-1) \cdot (-1) \cdot \sqrt{15} \pmod{F_n} = = 6 + 2\sqrt{15} \pmod{F_n} = (6+\sigma) \pmod{F_n}$

We chose σ such that $\omega = \frac{(6+\sigma)^2}{24}$. We can use this to compute $\omega^{\frac{F_n-1}{2}}$ in the group X :
$\omega^{\frac{F_n-1}{2}} = \frac{(6+\sigma)^{F_n-1}}{24^{\frac{F_n-1}{2}}} = \frac{(6+\sigma)^{F_n}}{(6+\sigma) \cdot 24^{\frac{F_n-1}{2}}} \equiv \frac{(6+\sigma)}{(6+\sigma)\cdot(-1)} \pmod{F_n} = -1 \pmod{F_n}$
where we use fact that :
$24^{\frac{F_n-1}{2}} = (2^{\frac{F_n-1}{2}})^3 \cdot (3^{\frac{F_n-1}{2}}) \equiv (1^3) \cdot (-1) \pmod{F_n} = -1 \pmod{F_n}$
So we have shown that :
$\omega^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}$

If we write this as $\omega^{\frac{2^{2^n}+1-1}{2}} = \omega^{2^{2^n-1}} = \omega^{2^{2^n-2}} \cdot \omega^{2^{2^n-2}} \equiv -1 \pmod{F_n}$,multiply both sides by $\bar{\omega}^{2^{2^n-2}}$, and put both terms on the left hand side to write this as : $\omega^{2^{2^n-2}} + \bar{\omega}^{2^{2^n-2}} \equiv 0 \pmod{F_n}$ $\omega^{2^{2(2^{n-1}-1)}} + \bar{\omega}^{2^{2(2^{n-1}-1)}} \equiv 0 \pmod{F_n} \Rightarrow S_{2^{n-1}-1} \equiv 0 \pmod{F_n}$

Since the left hand side is an integer this means therefore that $S_{2^{n-1}-1}$ must be divisible by $2^{2^n}+1$.

Proof of sufficiency

If $S_{2^{n-1}-1}$ is divisible by $2^{2^n}+1$, then $2^{2^n}+1$ is prime .

We rely on simplification of the proof of Lucas-Lehmer test by J. W. Bruce .If $2^{2^n}+1$ is not prime then it must be divisible by some prime factor F less than or equal to the square root of $2^{2^n}+1$. From the hypothesis $S_{2^{n-1}-1}$ is divisible by $2^{2^n}+1$ so $S_{2^{n-1}-1}$ is also multiple of F , so we can write : $\omega^{2^{2(2^{n-1}-1)}} + \bar{\omega}^{2^{2(2^{n-1}-1)}} = K \cdot F$, for some integer K . We can write this equality as : $\omega^{2^{2^n-2}} + \bar{\omega}^{2^{2^n-2}} = K \cdot F$ Note that $\omega \cdot \bar{\omega} = 1$ so we can multiply both sides by $\omega^{2^{2^n-2}}$ and rewrite this relation as : $\omega^{2^{2^n-1}} = K \cdot F \cdot \omega^{2^{2^n-2}} - 1$. If we square both sides we get : $\omega^{2^{2^n}} = (K \cdot F \cdot \omega^{2^{2^n-2}} - 1)^2$ Now consider the set of numbers $a + b\sqrt{15}$ for integers a and b where $a + b\sqrt{15}$ and $c + d\sqrt{15}$ are considered equivalent if a and c differ by a multiple of F , and the same is true for b and d . There are F^2 of these numbers , and addition and multiplication can be verified to be well-defined on sets of equivalent numbers. Given the element ω (considered as representative of an equivalence class) , the associative law allows us to use exponential notation for repeated products : $\omega^n = \omega \cdot \omega \cdots \omega$, where the product contains n factors and the usual rules for exponents can be justified . Consider the sequence of elements $\omega, \omega^2, \omega^3 \ldots$. Because ω has the inverse $\bar{\omega}$ every element in this sequence has an inverse . So there can be at most F^2-1 different elements of this sequence. Thus there must be at least two different exponents where $\omega^j = \omega^k$ with $j < k \leq F^2$. Multiply j times by inverse of ω to get that $\omega^{k-j} = 1$ with $1 \leq k-j \leq F^2-1$. So we have proven that ω satisfies $\omega^n = 1$ for some positive exponent n less than or equal to F^2-1 . Define the order of ω to be smallest positive integer d such that $\omega^d = 1$. So if n is any other positive integer satisfying $\omega^n = 1$ then n must be multiple of d . Write $n = q \cdot d + r$ with $r < d$. Then if $r \neq 0$ we have $1 = \omega^n = \omega^{q \cdot d + r} = (\omega^d)^q \cdot \omega^r = 1^q \cdot \omega^r = \omega^r$ contradicting the minimality of d so $r = 0$ and n is multiple of d . The relation $\omega^{2^{2^n}} = (K \cdot F \cdot \omega^{2^{2^n-2}} - 1)^2$ shows that $\omega^{2^{2^n}} \equiv 1 \pmod{F}$. So that 2^{2^n} must be multiple of the order of ω . But the relation

$\omega^{2^{2^n-1}} = K \cdot F \cdot \omega^{2^{2^n-2}} - 1$ shows that $\omega^{2^{2^n-1}} \equiv -1 \pmod F$ so the order cannot be any proper factor of 2^{2^n} , therefore the order must be 2^{2^n} . Since this order is less than or equal to $F^2 - 1$ and F is less or equal to the square root of $2^{2^n} + 1$ we have relation : $2^{2^n} \leq F^2 - 1 \leq 2^{2^n}$. This is true only if $2^{2^n} = F^2 - 1 \Rightarrow 2^{2^n} + 1 = F^2$. We will show that Fermat number cannot be square of prime factor .

Theorem : Any prime divisor p of $F_n = 2^{2^n} + 1$ is of the form $k \cdot 2^{n+2} + 1$ whenever n is greater than one .

So prime factor F must be of the form $k \cdot 2^{n+2} + 1$, therefore we can write : $2^{2^n} + 1 = (k \cdot 2^{n+2} + 1)^2$ $2^{2^n} + 1 = k^2 \cdot 2^{2n+4} + 2 \cdot k \cdot 2^{n+2} + 1$ $2^{2^n} = k \cdot 2^{n+3} \cdot (k \cdot 2^{n+1} + 1)$

The last equality cannot be true since $k \cdot 2^{n+1} + 1$ is an odd number and 2^{2^n} has no odd prime factors so $2^{2^n} + 1 \neq F^2$ and therefore we have relation $2^{2^n} < F^2 - 1 < 2^{2^n}$ which is contradiction so therefore $2^{2^n} + 1$ must be prime .

Q.E.D.

21 Prime number formula

$$p_n = 1 + \sum_{k=1}^{2\cdot(\lfloor n\ln(n)\rfloor+1)} \left(1 - \left\lfloor \frac{1}{n} \cdot \sum_{j=2}^{k} \left\lceil \frac{3 - \sum_{i=1}^{j} \left\lfloor \frac{\lfloor \frac{j}{i} \rfloor}{\lceil \frac{j}{i} \rceil} \right\rfloor}{j} \right\rceil \right\rfloor \right)$$

22 Primality criterion for specific class of $N = 3 \cdot 2^n - 1$

Definition 22.1. 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 22.1. *Let $N = 3 \cdot 2^n - 1$ such that $n > 2$ and $n \equiv 2 \pmod 4$*
Let $S_i = P_2(S_{i-1})$ with

$$S_0 = \begin{cases} P_3(32), & \text{if } n \equiv 2 \pmod 8 \\ P_3(36), & \text{if } n \equiv 6 \pmod 8 \end{cases}$$

thus , N is prime iff $S_{n-2} \equiv 0 \pmod N$

23 Probable prime tests for generalized Fermat numbers

Definition 23.1. 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 23.1. *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 .

Proof by mathlove . 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 $\alpha\beta = 1$,

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

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,

$$\alpha^N + \beta^N \equiv 2 \cdot 3^N \equiv 2 \cdot 3 \equiv 6 \pmod N \tag{3}$$

Similarly,

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

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

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

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),

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

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.

Q.E.D.

Theorem 23.2. *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 .

Proof by mathlove . First of all, we prove by induction that

$$S_i = p^{2b^{i+1}} + q^{2b^{i+1}} \tag{6}$$

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,

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

Similarly,

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

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

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

as desired.

Q.E.D.