A Lucas-Lehmer Type Primality Test for Numbers of the Form $4p^n - 1$

by Predrag Terzić

June 2, 2025

Abstract

We present a new, specific primality test for numbers of the form $N = 4p^n - 1$, where p is an odd prime and $n \geq 1$. The test is a generalization of the Lucas-Lehmer test for Mersenne numbers and relies on a sequence defined by Dickson polynomials. We prove that, under a certain condition, N is prime if and only if the n-th term of a specific sequence is congruent to zero modulo N. This provides a deterministic primality test for this family of numbers.

1 Introduction and Main Result

The Lucas-Lehmer test provides an efficient primality test for Mersenne numbers $(2^k - 1)$. This work extends the principle of that test to a different family of numbers. We define a sequence based on Dickson polynomials and use it to establish a necessary and sufficient condition for the primality of $N = 4p^n - 1$.

Definition 1.1 (Dickson Polynomials)**.** The k-th Dickson polynomial of the first kind, denoted $D_k(x, a)$, is defined by the recurrence relation

$$D_{k+2}(x, a) = xD_{k+1}(x, a) - aD_k(x, a)$$

with initial conditions $D_0(x, a) = 2$ and $D_1(x, a) = x$.

A key property of these polynomials is that for $x = u + a/u$, we have $D_k(x, a) = u^k + (a/u)^k$.

We define a sequence $\{S_i\}$ as follows:

$$S_0 = 6, \quad S_i = D_p(S_{i-1}, 1) \quad \text{for } i \geq 1. \tag{1}$$

Our main result is the following theorem.

Theorem 1.2 (Main Theorem)**.** *Let p be an odd prime and $n \geq 1$. Let $N = 4p^n - 1$. If the sequence $\{S_i\}$ is defined as above and $S_{n-1} \not\equiv 0 \pmod{N}$, then*

$$N \text{ is prime} \iff S_n \equiv 0 \pmod{N}.$$

2 Properties of the Sequence

To prove the main theorem, we first establish a closed-form expression for the terms of the sequence $\{S_i\}$.

Lemma 2.1. *The terms of the sequence* $\{S_i\}$ *are given by*

$$S_i = (\sqrt{2}+1)^{2p^i} + (\sqrt{2}-1)^{2p^i}.$$

Proof. We proceed by induction on i. For $i = 0$, we have

$$(\sqrt{2}+1)^2 + (\sqrt{2}-1)^2 = (2+2\sqrt{2}+1) + (2-2\sqrt{2}+1) = 3+2\sqrt{2}+3-2\sqrt{2} = 6 = S_0.$$

So the base case holds.

Now, assume the formula holds for S_{i-1}. Let $u = (\sqrt{2}+1)^{2p^{i-1}}$. Then $u^{-1} = ((\sqrt{2}+1)^{-1})^{2p^{i-1}} = (\sqrt{2}-1)^{2p^{i-1}}$. By the inductive hypothesis, $S_{i-1} = u + u^{-1}$.

Using the property of Dickson polynomials with $a = 1$, we have:

$$S_i = D_p(S_{i-1}, 1) = D_p(u + u^{-1}, 1) = u^p + u^{-p}.$$

Substituting the expression for u:

$$\begin{aligned} S_i &= \left((\sqrt{2}+1)^{2p^{i-1}}\right)^p + \left((\sqrt{2}-1)^{2p^{i-1}}\right)^p \\ &= (\sqrt{2}+1)^{2p^i} + (\sqrt{2}-1)^{2p^i}. \end{aligned}$$

This completes the induction. □

Lemma 2.2. *For* $N = 4p^n - 1$*, where* p *is an odd prime, the Jacobi symbol* $\left(\frac{2}{N}\right) = -1$.

Proof. Since p is an odd prime, p is congruent to $1, 3, 5$, or $7 \pmod 8$. Its powers p^n will also be odd. Let $p^n = 2k + 1$ for some integer $k \geq 1$. Then $N = 4(2k + 1) - 1 = 8k + 4 - 1 = 8k + 3$. By the properties of the Jacobi symbol, for any integer $m \equiv 3 \pmod 8$, we have $\left(\frac{2}{m}\right) = -1$. Therefore, $\left(\frac{2}{N}\right) = -1$. □

Remark 2.3. Lemma 2.2 implies that 2 is a quadratic non-residue modulo any prime factor of N. This justifies performing arithmetic in the finite field extension $\mathbb{Z}_N(\sqrt{2})$, which is isomorphic to $\mathbb{F}_{N^2}$ if N is prime.

3 Proof of the Main Theorem

Let $\alpha = \sqrt{2} + 1$. Then $\alpha^{-1} = \sqrt{2} - 1$. The sequence term S_n can be written as $S_n = \alpha^{2p^n} + \alpha^{-2p^n}$.

3.1 Proof of Necessity ($\Longrightarrow$)

Assume $N = 4p^n - 1$ is a prime number. We must show that $S_n \equiv 0 \pmod N$.

We work in the finite field $\mathbb{Z}_N(\sqrt{2}) \cong \mathbb{F}_{N^2}$. We use the Frobenius automorphism, which states that $x^N = x$ for $x \in \mathbb{Z}_N$ and $(a + b\sqrt{2})^N \equiv a^N + b^N(\sqrt{2})^N \pmod N$. By

Fermat's Little Theorem, $a^N \equiv a \pmod{N}$ and $b^N \equiv b \pmod{N}$. By Euler's criterion and Lemma 2.2:

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

Applying this to $\alpha = 1 + \sqrt{2}$:

$$\alpha^N = (1+\sqrt{2})^N \equiv 1^N + (\sqrt{2})^N \equiv 1 - \sqrt{2} \pmod{N}.$$

Note that $1 - \sqrt{2} = -(\sqrt{2} - 1) = -\alpha^{-1}$. So we have the key relation $\alpha^N \equiv -\alpha^{-1} \pmod{N}$.

Now, we use this to evaluate α^{N+1}:

$$\alpha^{N+1} = \alpha \cdot \alpha^N \equiv \alpha \cdot (-\alpha^{-1}) = -1 \pmod{N}.$$

Since $N + 1 = (4p^n - 1) + 1 = 4p^n$, we have:

$$\alpha^{4p^n} \equiv -1 \pmod{N}.$$

This can be rewritten as $\alpha^{4p^n} + 1 \equiv 0 \pmod{N}$. Since α is invertible, we can divide by α^{2p^n}:

$$\alpha^{2p^n} + \alpha^{-2p^n} \equiv 0 \pmod{N}.$$

By Lemma 2.1, the left side is exactly S_n. Therefore, $S_n \equiv 0 \pmod{N}$.

3.2 Proof of Sufficiency ($\Longleftarrow$)

Assume $S_n \equiv 0 \pmod{N}$ and $S_{n-1} \not\equiv 0 \pmod{N}$. We must show that N is prime.

Let q be any prime divisor of N. All congruences modulo N must also hold modulo q. The condition $S_n \equiv 0 \pmod{q}$ means $\alpha^{2p^n} + \alpha^{-2p^n} \equiv 0 \pmod{q}$. Multiplying by α^{2p^n} yields $\alpha^{4p^n} + 1 \equiv 0 \pmod{q}$, which implies:

$$\alpha^{4p^n} \equiv -1 \pmod{q}. \tag{2}$$

Squaring this gives:

$$\alpha^{8p^n} \equiv 1 \pmod{q}. \tag{3}$$

Let $k = \text{ord}_q(\alpha)$ be the order of α in the multiplicative group of the field $\mathbb{Z}_q(\sqrt{2})$. From (3), k must divide $8p^n$. From (2), k cannot divide $4p^n$. This implies that the highest power of 2 dividing k is exactly $2^3 = 8$.

Now consider the condition $S_{n-1} \not\equiv 0 \pmod{N}$, which implies $S_{n-1} \not\equiv 0 \pmod{q}$. This means $\alpha^{2p^{n-1}} + \alpha^{-2p^{n-1}} \not\equiv 0 \pmod{q}$, which implies $\alpha^{4p^{n-1}} \not\equiv -1 \pmod{q}$. This tells us that k does not divide $8p^{n-1}$. If it did, then since we know $v_2(k) = 3$, k would divide $8p^{n-1}$ but not $4p^{n-1}$, which would mean $\alpha^{4p^{n-1}} \equiv -1 \pmod{q}$. This is a contradiction.

So, the order k divides $8p^n$ but does not divide $8p^{n-1}$. This means that the highest power of p dividing k must be p^n. Combining our findings, the order of α modulo q is exactly $k = 8p^n$.

By Lagrange's theorem, the order of an element must divide the order of the group. The group is $(\mathbb{Z}_q(\sqrt{2}))^\times$, which has order $q^2 - 1$. Therefore, we must have $8p^n \mid (q^2 - 1)$.

Now, suppose for the sake of contradiction that N is composite. Then N must have a prime factor q such that $q \leq \sqrt{N}$. This leads to $q^2 \leq N = 4p^n - 1$.

From $8p^n \mid (q^2 - 1)$, we can write $q^2 - 1 = m \cdot 8p^n$ for some positive integer $m \geq 1$. This gives $q^2 = 8mp^n + 1$.

Combining the two inequalities for q^2:

$$8mp^n + 1 \leq 4p^n - 1$$

$$8mp^n \leq 4p^n - 2$$

$$m \leq \frac{4p^n - 2}{8p^n} = \frac{1}{2} - \frac{1}{4p^n}.$$

Since $p \geq 3$ and $n \geq 1$, the term $1/(4p^n)$ is positive. The inequality implies $m < 1/2$. However, m must be a positive integer. This is a contradiction.

The assumption that N has a prime factor $q \leq \sqrt{N}$ must be false. This means N has no prime factors other than itself, and therefore N must be prime. This completes the proof of the theorem. □

4 Conclusion

The theorem provides a deterministic primality test for the entire family of numbers $N = 4p^n - 1$. This result is an elegant instance of the general theory of Lucas-Lehmer type tests, which have been developed for numbers of the form $A \cdot B^n \pm 1$. The specific choice of the base sequence ($S_0 = 6$) provides the necessary properties for the argument to hold for this particular number form. This demonstrates how a general number-theoretic framework can be applied to produce a simple and definitive test for a specific case.