A Primality Criterion for Wagstaff Numbers

Predrag Terzić

August 13, 2025

Abstract

This document provides a complete proof of a primality test for Wagstaff numbers $W_p = (2^p + 1)/3$, where p is an odd prime. The test connects the primality of W_p to a divisibility property of a specific term in a Lucas sequence. We will prove both the necessity and sufficiency of the condition.

1 The Conjecture

Conjecture 1. *For an odd prime p, let W_p be the Wagstaff number*

$$W_p = \frac{2^p + 1}{3}$$

and let an index n be defined as

$$n = \frac{2^{p-2} + 1}{3}$$

Let $(V_k)_{k\geq 0}$ be the Lucas sequence defined by the recurrence relation

$$V_0 = 2, \quad V_1 = 6, \quad V_k = 6V_{k-1} - V_{k-2} \text{ for } k \geq 2.$$

Then W_p is prime if and only if W_p divides V_n.

$$W_p \text{ is prime} \iff W_p | V_n.$$

2 The Lucas Sequence (V_k)

The recurrence relation $V_k = 6V_{k-1} - V_{k-2}$ has the characteristic equation $x^2 - 6x + 1 = 0$. The roots of this equation are

$$x = \frac{6 \pm \sqrt{36 - 4}}{2} = 3 \pm 2\sqrt{2}.$$

Let $\alpha = 3 + 2\sqrt{2}$ and $\beta = 3 - 2\sqrt{2}$. Note that $\alpha\beta = 1$. The closed-form solution for the sequence is $V_k = A\alpha^k + B\beta^k$. Using the initial conditions:

$$V_0 = 2 \Rightarrow A + B = 2$$
$$V_1 = 6 \Rightarrow A\alpha + B\beta = 6$$

Solving these equations gives $A = 1$ and $B = 1$. Thus, the closed-form for the sequence is

$$V_k = \alpha^k + \beta^k = (3 + 2\sqrt{2})^k + (3 - 2\sqrt{2})^k.$$

It is also useful to note that $\alpha = (1 + \sqrt{2})^2$ and $\beta = (1 - \sqrt{2})^2$. Therefore,

$$V_k = (1 + \sqrt{2})^{2k} + (1 - \sqrt{2})^{2k}.$$

3 Proof of Necessity ($\Rightarrow$)

Proof. We assume that $N = W_p$ is a prime number and must show that $N|V_n$, which is equivalent to showing $V_n \equiv 0 \pmod{N}$.

First, we determine the quadratic character of 2 modulo N. Since p is an odd prime, $p \geq 3$. We have $3N = 2^p + 1$. For $p \geq 3$, 2^p is divisible by 8, so $2^p + 1 \equiv 1 \pmod{8}$, which gives $3N \equiv 1 \pmod{8}$. Multiplying by 3 (the inverse of 3 mod 8), we get $N \equiv 3 \pmod{8}$.

By the law of quadratic reciprocity, the Legendre symbol is $(\frac{2}{N}) = -1$. This means 2 is a quadratic non-residue modulo N, and the ring $\mathbb{Z}_N[\sqrt{2}]$ is a finite field $\mathbb{F}_{N^2}$. In the field $\mathbb{F}_{N^2}$, for any element $x = a + b\sqrt{2}$, we have the identity $x^N \equiv \overline{x}$, where $\overline{x} = a - b\sqrt{2}$ is the conjugate.

Applying this to $\alpha = 3 + 2\sqrt{2}$, we get $\alpha^N \equiv 3 - 2\sqrt{2} = \beta \pmod{N}$. Since $\alpha\beta = 1$, we have $\beta = \alpha^{-1}$, which implies $\alpha^{N+1} \equiv 1 \pmod{N}$.

The index n is related to N by the formula $4n = N + 1$. We use this to analyze $\alpha^{(N+1)/2}$. Since $\alpha = (1 + \sqrt{2})^2$, we have:

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

The term $V_{(N+1)/2}$ of the sequence is $V_{(N+1)/2} = \alpha^{(N+1)/2} + \beta^{(N+1)/2} \equiv -1 + (-1) = -2 \pmod{N}$.

Using the identity $V_{2k} = V_k^2 - 2$ with $k = n = (N+1)/4$, we get $V_{(N+1)/2} = V_{2n} = V_n^2 - 2$. Combining our results, we have $V_n^2 - 2 \equiv -2 \pmod{N}$, which simplifies to $V_n^2 \equiv 0 \pmod{N}$. As N is prime, this implies N must divide V_n. □

4 Proof of Sufficiency ($\Leftarrow$)

Proof. We assume that $N|V_n$, where $N = W_p$, and we want to prove that N is prime. The proof is by contradiction.

Assume that N is composite. Let q be any prime factor of N. From the condition $N|V_n$, it follows that $q|V_n$, so $V_n \equiv 0 \pmod{q}$.

$$\alpha^n + \beta^n \equiv 0 \pmod{q}.$$

Multiplying by α^n (which is invertible in $\mathbb{Z}_q[\sqrt{2}]$) we get:

$$\alpha^{2n} + 1 \equiv 0 \pmod{q} \implies \alpha^{2n} \equiv -1 \pmod{q}.$$

Squaring this gives $\alpha^{4n} \equiv 1 \pmod{q}$.

Let d be the order of α in the multiplicative group of the ring $\mathbb{Z}_q[\sqrt{2}]$. The congruences above show that d must divide $4n$, but d cannot divide $2n$. Before proceeding, we must rigorously prove that these conditions imply the order d is exactly $4n$.

Lemma 1. *If $V_n \equiv 0 \pmod{q}$, where q is a prime factor of $N = W_p$, then the order of $\alpha = 3 + 2\sqrt{2}$ in the multiplicative group of the ring $\mathbb{Z}_q[\sqrt{2}]$ is exactly $4n$.*

Proof. Let d be the order of α in the multiplicative group of the ring $\mathbb{Z}_q[\sqrt{2}]$, denoted as $\text{ord}_q(\alpha)$. We must show that $d = 4n$.

Step 1: Initial Derivations from the Premise

We are given the condition $V_n \equiv 0 \pmod{q}$. By the Binet form of the sequence, $V_n = \alpha^n + \beta^n$, where $\beta = 3 - 2\sqrt{2} = \alpha^{-1}$.

$$\begin{aligned} \alpha^n + \beta^n &\equiv 0 \pmod{q} \\ \alpha^n + \alpha^{-n} &\equiv 0 \pmod{q} \end{aligned}$$

Since α is invertible in the ring $\mathbb{Z}_q[\sqrt{2}]$, we can multiply the congruence by α^n:

$$\begin{aligned} \alpha^n(\alpha^n + \alpha^{-n}) &\equiv \alpha^n \cdot 0 \pmod{q} \\ \alpha^{2n} + 1 &\equiv 0 \pmod{q} \\ \alpha^{2n} &\equiv -1 \pmod{q} \end{aligned}$$

This result is fundamental. Squaring both sides gives:

$$\begin{aligned} (\alpha^{2n})^2 &\equiv (-1)^2 \pmod{q} \\ \alpha^{4n} &\equiv 1 \pmod{q} \end{aligned}$$

From these two congruences, we can deduce two facts about the order d:

1. Since $\alpha^{4n} \equiv 1 \pmod{q}$, the order d must be a divisor of $4n$.
2. Since $\alpha^{2n} \equiv -1 \not\equiv 1 \pmod{q}$, the order d cannot be a divisor of $2n$.

Step 2: Proof by Contradiction

Assume, for the sake of contradiction, that the order d is **not** $4n$. Since $d|4n$ and $d \nmid 2n$, the highest power of 2 dividing d must be the same as the highest

power of 2 dividing $4n$. For an odd prime $p \geq 3$, the index $n = (2^{p-2} + 1)/3$ is an odd integer. Therefore, the prime factorization of $4n$ contains exactly two factors of 2 (i.e., 2^2). This implies that d must be a multiple of 4.

Our assumption that d is a proper divisor of $4n$ means we can write $d = 4m$ for some integer m that is a **proper divisor** of n. Our goal is to show this leads to a contradiction.

Step 3: Reaching the Contradiction

If the order of α is $d = 4m$, then the order of the element $x = \alpha^m$ must be exactly 4. In any ring, an element of order 4 must satisfy $x^2 \equiv -1$. Therefore, our assumption directly implies:

$$(\alpha^m)^2 \equiv -1 \pmod{q} \implies \alpha^{2m} \equiv -1 \pmod{q}$$

From this, we can deduce a fact about the sequence term V_m:

$$\begin{aligned} \alpha^{2m} + 1 &\equiv 0 \pmod{q} \\ \alpha^m(\alpha^m + \alpha^{-m}) &\equiv 0 \pmod{q} \end{aligned}$$

Since α^m is invertible, we can divide by it:

$$\alpha^m + \alpha^{-m} \equiv 0 \pmod{q} \implies \alpha^m + \beta^m \equiv 0 \pmod{q} \implies V_m \equiv 0 \pmod{q}$$

So, the assumption that the order is $4m$ (for m a proper divisor of n) forces the conclusion that V_m must also be divisible by q.

This is where we find the contradiction, by using the concept of the rank of apparition.

Definition (Rank of Apparition)**.** For the sequence (V_k) and a prime q, the **rank of apparition** is the smallest positive integer k_0 such that $V_{k_0} \equiv 0 \pmod{q}$.

Let n_0 be the rank of apparition for q in the sequence (V_k).

1. Our initial premise is $V_n \equiv 0 \pmod{q}$. By the Law of Apparition for this sequence (see Appendix), this implies that n must be an odd multiple of the rank of apparition, n_0. So, $n = j \cdot n_0$ for some odd integer $j \geq 1$.
2. Our contradictory assumption (that $\text{ord}_q(\alpha) = 4m$ for m a proper divisor of n) led us to the conclusion that $V_m \equiv 0 \pmod{q}$.
3. This implies that m must also be an odd multiple of the same rank of apparition n_0. So, $m = j' \cdot n_0$ for some odd integer $j' \geq 1$.
4. However, m is a **proper divisor** of n. This means $m < n$.
5. Combining these facts, we have $j' \cdot n_0 < j \cdot n_0$, which implies $j' < j$.

This does not immediately present a contradiction. However, let's consider the smallest positive integer k for which $V_k \equiv 0 \pmod{q}$, which is n_0 by definition. Our initial premise was $V_n \equiv 0 \pmod{q}$. If we had started with the rank of apparition n_0 instead of n, the argument would be:

- Assume, for contradiction, that the order of α is not $4n_0$, but rather $4m_0$ where m_0 is a proper divisor of n_0.
- This assumption leads to the conclusion that $V_{m_0} \equiv 0 \pmod{q}$.
- But m_0 is a proper divisor of n_0, which means $m_0 < n_0$. This contradicts the definition of n_0 as the *smallest* positive integer for which the sequence term is divisible by q.

Therefore, the assumption that the order can be a smaller value $4m$ must be false. The only remaining possibility is that the order is exactly $4n$. □

With the lemma proven, we now know that the order of α is $d = 4n$. We proceed with the main proof by examining the two cases for the quadratic character of 2 modulo q.

Part 1 (Case 1: $(\frac{2}{q}) = 1$.)**.** *In this case, $\sqrt{2}$ exists in $\mathbb{Z}_q$, so α is an element of the multiplicative group $\mathbb{Z}_q^\times$, which has order $q-1$. The order of α, $d = 4n$, must divide the order of the group.*

$$4n | q - 1.$$

This implies $q - 1 = j(4n)$ for some integer $j \geq 1$, so $q \geq 4n + 1$. Substituting $4n = N + 1$, we get:

$$q \geq (N + 1) + 1 = N + 2.$$

A prime factor q of a number N must be less than or equal to N. The result $q \geq N + 2$ is a contradiction. Therefore, N cannot have any prime factor q for which $(\frac{2}{q}) = 1$.

Part 2 (Case 2: $(\frac{2}{q}) = -1$.)**.** *In this case, $\mathbb{Z}_q[\sqrt{2}]$ is a field extension $\mathbb{F}_{q^2}$. The multiplicative group of this field has order $q^2 - 1$, and the order of α, $d = 4n$, must divide it.*

$$4n | q^2 - 1.$$

This implies $q^2 \geq 4n + 1$. Substituting $4n = N + 1$:

$$q^2 \geq N + 1.$$

From Case 1, we know any prime factor q of N must satisfy $(\frac{2}{q}) = -1$. If N is composite, its smallest prime factor q must satisfy $q \leq \sqrt{N}$, which implies $q^2 \leq N$. We now have two conflicting inequalities:

$$N \geq q^2 \geq N + 1.$$

This simplifies to $N \geq N + 1$, or $0 \geq 1$, which is impossible. The initial assumption that N is composite must be false. Therefore, $N = W_p$ must be a prime number.

□

A The Law of Apparition for the Sequence V_k

Property 1. *Let n_0 be the rank of apparition for a prime q in the sequence (V_k). Then $V_k \equiv 0 \pmod{q}$ if and only if $k = j \cdot n_0$ for some odd integer j.*

Proof. We prove the two directions separately.

Part 1: "If" direction ($\Leftarrow$)

Assume $k = j \cdot n_0$ for some odd integer j. We want to show $V_k \equiv 0 \pmod{q}$. We use the known Lucas sequence identity: $V_{jm} = L_j(V_m, 1)$, where $L_j(x, y)$ is the j-th Lucas polynomial. For $y = 1$, when j is odd, $L_j(x, 1)$ is a polynomial in x where every term has a factor of x. For example, $L_3(x, 1) = x^3 - 3x$. This means that if V_{n_0} is a factor of the expression for $V_{j \cdot n_0}$. Since we are given that $V_{n_0} \equiv 0 \pmod{q}$, it follows that $V_{j \cdot n_0} \equiv 0 \pmod{q}$. Thus, $V_k \equiv 0 \pmod{q}$.

Part 2: "Only if" direction ($\Rightarrow$)

Assume $V_k \equiv 0 \pmod{q}$. We must show that k is an odd multiple of n_0. The condition $V_k \equiv 0 \pmod{q}$ implies $\alpha^{2k} \equiv -1 \pmod{q}$. By definition of n_0, we also have $\alpha^{2n_0} \equiv -1 \pmod{q}$. Let $d_2 = \mathrm{ord}_q(\alpha^2)$. From $\alpha^{2n_0} \equiv -1$, we get $(\alpha^2)^{n_0} \equiv -1$, which implies $(\alpha^2)^{2n_0} \equiv 1 \pmod{q}$. Since n_0 is the *smallest* index for which $V_{n_0} \equiv 0$, d_2 must be exactly $2n_0$.

From $V_k \equiv 0 \pmod{q}$, we have $(\alpha^2)^k \equiv -1 \pmod{q}$. We also have $(\alpha^2)^{n_0} \equiv -1 \pmod{q}$. Therefore, $(\alpha^2)^k \equiv (\alpha^2)^{n_0} \pmod{q}$, which implies $(\alpha^2)^{k-n_0} \equiv 1 \pmod{q}$. This means the order $d_2 = 2n_0$ must divide the exponent $k - n_0$.

$$2n_0 \mid (k - n_0) \implies k - n_0 = c \cdot 2n_0 \text{ for some integer } c.$$

$$k = n_0 + c \cdot 2n_0 = n_0(1 + 2c).$$

Let $j = 1 + 2c$. By definition, j is an odd integer. Thus, $k = j \cdot n_0$ for some odd integer j. □