

# THE BPSW CONJECTURE

**Samuel S. Wagstaff, Jr.**[1]
*Center for Education and Research in Information Assurance and Security*
and
*Department of Computer Sciences, Purdue University, West Lafayette, Indiana*
ssw@cerias.purdue.edu

*Received: 5/6/26, Revised: 9/1/26, Accepted: 11/4/26, Published: 11/23/26*

**Abstract**

We prove a theorem about the primitive parts of the Fibonacci numbers and use it to search for a counterexample to the BPSW conjecture about probable primes and Lucas probable primes.

## 1. Introduction

A (Fermat) *base-a probable prime*, or prp($a$), is a positive integer $n$ that satisfies the conclusion of Fermat's little theorem. If $n$ is prime and $(a, n) = 1$, then

$$a^{n-1} \equiv 1 \pmod{n}. \tag{1}$$

A *base-a pseudoprime*, or psp($a$), is a *composite* $n$ that satisfies Congruence (1). If $n$ is odd, then we can write $n - 1 = d \cdot 2^s$ where $d$ is odd. If $n$ is an odd prime and $(a, n) = 1$, then either

$$a^{d} \equiv 1 \pmod{n}, \quad \text{or} \tag{2}$$

$$a^{d \cdot 2^r} \equiv -1 \pmod{n}, \quad \text{for some } r \text{ with } 0 \le r < s. \tag{3}$$

If either Congruence (2) or (3) is true, then $n$ is called a *base-a strong probable prime* (sprp($a$)). If either of these holds, then we also have $a^{n-1} = a^{d \cdot 2^s} \equiv 1 \pmod{n}$, so $n$ is a probable prime to base $a$. If neither Congruence (2) nor (3) holds, then $n$ is composite. If $n$ is composite and either Congruence (2) or (3) is true, then $n$ is called a *base-a strong pseudoprime* (spsp($a$)).

Let $D$, $P$ and $Q$ be integers with $P > 0$ and $D = P^2 - 4Q \neq 0$. Define $U_0 = 0$, $U_1 = 1$, $V_0 = 2$ and $V_1 = P$. The Lucas sequences $U_k$ and $V_k$ with parameters $D$, $P$ and $Q$ are defined recursively for $k \ge 2$ by

$$U_k(P, Q) = U_k = PU_{k-1} - QU_{k-2} \quad \text{and} \quad V_k(P, Q) = V_k = PV_{k-1} - QV_{k-2}\,.$$

DOI: 10.5281/zenodo.24473693
[1]This work was supported by the CERIAS Center at Purdue University

Let $n$ be an odd positive integer and write $\epsilon(n)$ for the Jacobi symbol $(D/n)$. It is known [2, pp. 1391-1392], [3, Theorem 8] that if $n$ is prime and $(n, Q) = 1$, then

$$U_{n-\epsilon(n)} \equiv 0 \pmod{n}, \tag{4}$$

We choose an algorithm for picking $D$, $P$, and $Q$ based on $n$. Since $(D/n) = 1$ would be just like a pseudoprime test (see [8]), we require that the Jacobi symbol $(D/n) = -1$. If $n$ is prime, $(n, D) = (n, Q) = 1$, and $(D/n) = -1$, then $n - \epsilon(n) = n + 1$ and Congruence (4) becomes

$$U_{n+1} \equiv 0 \pmod{n}. \tag{5}$$

If $n$ satisfies Congruence (5), then $n$ is called a *Lucas probable prime* with parameters $P$ and $Q$, written lprp($P$, $Q$). If $n$ satisfies Congruence (5) and we know it is composite, then we call $n$ a *Lucas pseudoprime*, written lpsp($P$, $Q$). If $n$ fails (5), then $n$ is composite.

The precise sequence of numbers that turn out to be Lucas pseudoprimes depends on the algorithm for choosing $D$, $P$, and $Q$. One algorithm, first proposed by John Selfridge in [8] and mentioned in [2], and which seems to be widely used in primality testing, is this one.

**Method 1.** Let $D$ be the first element of the sequence $5, -7, 9, -11, 13, -15, \ldots$ for which $(D/n) = -1$. Let $P = 1$ and $Q = (1 - D)/4$.

This algorithm never sets $Q = 1$, but if $D = 5$, it sets $Q = -1$. (Method 1 sets $Q = -1$ fairly often, namely, when $n \equiv \pm 2 \pmod{5}$.) An alternate method is this one. See [2] for why it might be better.

**Method 2.** Choose $D$, $P$, and $Q$ as in Method 1 above. If $Q = -1$, change both $P$ and $Q$ to 5.

Method 2 leaves $D = P^2 - 4Q$ unchanged from Method 1. If $n$ is odd, then we can write $n + 1 = d \cdot 2^s$ where $d$ is odd. If $n$ is prime, $(D/n) = -1$, and $(a, n) = 1$, then we will have either

$$U_d \equiv 0 \pmod{n}, \quad \text{or} \tag{6}$$

$$V_{d \cdot 2^r} \equiv 0 \pmod{n}, \quad \text{for some } r \text{ with } 0 \le r < s. \tag{7}$$

If $n$ satisfies Congruence (6) or (7), then $n$ is called a *strong Lucas probable prime* with parameters $P$ and $Q$, written slprp($P$, $Q$). If $n$ is an slprp($P$, $Q$), then $n$ is also an lprp($P$, $Q$), so that $U_{n+1} = U_{d \cdot 2^s} \equiv 0 \pmod{n}$ because $U_{2k} = U_k V_k$ for all $k$. If $n$ satisfies Congruence (6) or (7) and is *composite*, then $n$ is called a *strong Lucas pseudoprime*, written slpsp($P$, $Q$). It is proved in the Appendix of [1] that the Lucas pseudoprimes generated by Methods 1 and 2 are the same. The same statement is true for strong Lucas pseudoprimes.

We need a few more definitions for $b^n - 1$ and Lucas sequences. It turns out that if $m$ is a positive integer relatively prime to $Q$, then there is a positive integer $n$

for which $m \mid U_n$. In this case, we write $\omega(m)$ for the least positive integer $n$ with $m \mid U_n$, called the *rank of apparition of* $m$. It is known [11, Theorem 4.5.4] that if $m$ is relatively prime to $Q$ and $m \mid U_n$, then $\omega(m) \mid n$. A prime factor $p$ of $b^n - 1$ is called *primitive* if it does not divide $b^m - 1$ for any $0 < m < n$. A primitive prime factor $p$ of $b^n - 1$ is called *intrinsic* if $p \mid n$. The *primitive part of* $b^n - 1$ is the product of the primitive prime factors of $b^n - 1$. A prime factor $p$ of $U_n$ is called *primitive* if $\omega(p) = n$. A primitive prime factor $p$ of $U_n$ is called *intrinsic* if $p \mid n$. It is known (see the proof of Theorem 4.5.10 in [11]) that if $p$ is an odd non-intrinsic primitive factor of $U_n$, then $p \equiv \epsilon(p) \pmod{n}$. All primitive prime factors of $U_n$ have the same rank of apparition $n$. The *primitive part of* $U_n$ is the product of the primitive prime factors of $U_n$.

## 2. The BPSW Primality Test and Conjecture

In [2], it is shown that we get an effective test for primality by combining Fermat and Lucas probable prime tests. They conjectured that the test was infallible. The authors of [8] and [2] observed that, up to $25 \cdot 10^9$, there was no overlap between the psp(2) and the lpsp from Method 2. Further, no one has reported a larger composite $n$ that is both psp(2) and lpsp($P$, $Q$) using Method 1 or 2. A reward of \$620 [1] was offered for either a proof of the conjecture that no composite is both a strong base 2 pseudoprime and a Lucas pseudoprime, or an example of a composite declared prime by this test. No one has claimed the reward after 45 years; many have tried to collect it. It has been tested on billions of large odd integers $n$ and has never been reported to have failed. Using the list of psp(2) $< 2^{64}$ in Feitsma [5] we found that none of these numbers is an lpsp. A Carmichael number is a positive integer $n$ which is psp($b$) for every $0 < b < n$ with $\gcd(b, n) = 1$. In 2025, using the list of Carmichael numbers computed by Shallue and Webster [9], Baillie found that no Carmichael number $< 10^{24}$ is an lpsp. See Pomerance [7] for a heuristic argument that there probably are many counterexamples to the conjecture, and how one might collect the reward. (His argument constructs Carmichael numbers that are lpsp.) The numbers in this argument are very large, suggesting that the smallest counterexample might be rather large.

## 3. Fibonacci Numbers

This section introduces the tools we will use to search for a counterexample to the BPSW conjecture. We study the Fibonacci and Lucas numbers. Let $P = 1$, $Q = -1$, and $D = 5$. For these special Lucas sequences we write $F_n = U_n$ and $L_n = V_n$. Note that $\epsilon(n) = (5/n) = 0$ when $5 \mid n$, $\epsilon(n) = 1$ when $n \equiv \pm 1 \pmod 5$, and $\epsilon(n) = -1$ when $n \equiv \pm 2 \pmod 5$. The Fibonacci numbers are a divisibility sequence [11], which means that if $m \mid n$, then $F_m \mid F_n$.

See [10, Corollary 4.5] for a proof of the next result.

**Theorem 1.** ([10]) *For every integer $b > 1$ and integer $m > 2$, every composite divisor of the primitive part of $b^m - 1$ or $b^m + 1$, with any intrinsic factor removed, is a strong pseudoprime to base $b$.*

Note that the primitive part of $b^m + 1$ is the same as the primitive part of $b^{2m} - 1$ because $b^{2m} - 1 = (b^m - 1)(b^m + 1)$ for all $m$.

The next theorem is the analogue of Theorem 1 for Fibonacci numbers. Theorem 1.1 of Greene et al. [6] is a similar result.

**Theorem 2.** *For every integer $m > 5$, every composite divisor $n \equiv \pm 2 \pmod 5$ of the primitive part of $F_m$ or $L_m$, with any intrinsic factor removed, is a strong Lucas pseudoprime.*

*Proof.* Note first that, since $n \equiv \pm 2 \pmod 5$, both Method 1 and Method 2 choose $D = 5$. We consider only Method 1, where the Lucas sequence is the Fibonacci numbers, because the (strong) Lucas pseudoprimes are the same for Methods 1 and 2 [1, Appendix].

Let $p_1, p_2, \ldots, p_r$ be the prime factors of $n$, perhaps with repetition. Then $r > 1$ since $n$ is composite. No $p_i$ is 2 because $F_3 = 2$ and $L_0 = 2$, so 2 cannot divide the primitive part of $F_m$ or $L_m$ with $m > 5$. No $p_i$ is 5 because $n \equiv \pm 2 \pmod 5$. The number of $p_i \equiv \pm 2 \pmod 5$ must be odd since $n \equiv \pm 2 \pmod 5$. Since the $p_i$ are primitive divisors of $F_m$, they all have the same rank of apparition $\omega(p_i) = m$.

By Equation (4.3.3) of [11], $p_i \mid F_{p_i - \epsilon(p_i)}$. Therefore, $m = \omega(p_i) \mid p_i - \epsilon(p_i)$ or $p_i \equiv \epsilon(p_i) \pmod m$. Thus, $n = \prod p_i \equiv \prod \epsilon(p_i) \pmod m$. There is an odd number of $p_i \equiv \pm 2 \pmod 5$, so $\prod \epsilon(p_i) \equiv -1 \pmod m$. Hence, $m \mid n + 1$. Since the Fibonacci numbers are a divisibility sequence, $F_m \mid F_{n+1}$. But $n \mid F_m$, so $n \mid F_{n+1}$ and thus $n$ is a Lucas pseudoprime by Congruence (5).

Since $n$ is odd, we can write $n + 1 = d \cdot 2^s$ where $d$ is odd and $s > 0$. Let $r$ be the smallest integer for which $n$ divides $F_{d \cdot 2^r}$. If $r = 0$, then $n$ divides $F_d$ and $n$ is a strong Lucas pseudoprime by Congruence (6). Otherwise, $0 < r \leq s$. Recall that all prime factors of $n$ have the same rank of apparition $m$. Therefore, every $p_i$ divides $F_{d \cdot 2^r}$ and no $p_i$ divides $F_{d \cdot 2^{r-1}}$. Since $F_{2k} = F_k L_k$ for all $k$, and $n$ divides $F_{d \cdot 2^r}$ but not $F_{d \cdot 2^{r-1}}$, $n$ must divide $L_{d \cdot 2^{r-1}}$ and $n$ is a strong Lucas pseudoprime by Congruence (7). The primitive part of $L_m$ is the same as the primitive part of $F_{2m}$ because $F_{2m} = F_m L_m$ for all $m$. This completes the proof. □

## 4. The Search

We searched for a possible counterexample to the BPSW conjecture using Theorems 1 and 2 as sources of thousands of numbers, most rather large, that satisfy one of the two conditions of a counterexample. The hope is that, since these numbers need to satisfy just one more condition to be a counterexample, we might find a counterexample by testing them.

Using Theorem 1, we computed the primitive parts of many $b^m - 1$ and $b^m + 1$, with any intrinsic factor removed, and tested whether they were (strong) Lucas probable primes. If the number was a strong Lucas probable prime, we tested it for probable primality by strong probable prime tests to bases 101 and 137. If it passed these two strong probable prime tests, we assumed it was prime. Otherwise, we have a counterexample.

We performed similar computations with the primitive parts congruent to $\pm 2 \pmod 5$ of $F_m$ and $L_m$ using Theorem 2 and a probable prime test to base 2. If the number was a strong probable prime to base 2, we tested it for probably primality by strong probable prime tests to bases 101 and 137. If it passed these two strong probable prime tests, we assumed it was prime. Otherwise, we have a counterexample. Greene et al. [6] made a similar search for a BPSW counterexample using all known composite $n \mid F_m$ with $n \equiv \pm 2 \pmod 5$ for all $m < 10000$ as well as all prime $m < 100000$.

We tested $b^m - 1$ for all $m$ between 1 and 100000 and found no counterexample. Earlier, Baillie tested all primes $p < 120000$ and found that $2^p - 1$ is a Lucas probable prime only when it is a Mersenne prime. His result inspired this paper. The tests for $F_m$ were faster because we considered only primitive parts congruent to $\pm 2 \pmod 5$, so we tested all $m < 300000$ and found no counterexample. A byproduct of the computation was lists of the $m < 100000$, 50000, 300000, or 150000 for which the primitive part of $b^m - 1$, $b^m + 1$, $F_m$, or $L_m$, respectively, is prime or probably prime.

The $m$ for $b^m - 1$ (which include the Mersenne prime exponents) are 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 24, 26, 27, 30, 31, 32, 33, 34, 38, 40, 42, 46, 49, 54, 56, 61, 62, 65, 69, 77, 78, 80, 85, 86, 89, 90, 93, 98, 107, 120, 122, 126, 127, 129, 133, 145, 147, 150, 158, 165, 170, 174, 184, 192, 195, 202, 208, 234, 254, 261, 280, 296, 312, 322, 334, 342, 345, 366, 374, 382, 398, 410, 414, 425, 447, 471, 507, 521, 550, 567, 579, 590, 600, 602, 607, 626, 690, 694, 712, 745, 795, 816, 889, 897, 909, 954, 990, 1106, 1192, 1224, 1230, 1279, 1384, 1386, 1402, 1464, 1512, 1554, 1562, 1600, 1670, 1683, 1727, 1781, 1834, 1904, 1990, 1992, 2008, 2037, 2203, 2281, 2298, 2353, 2406, 2456, 2499, 2536, 2838, 3006, 3074, 3217, 3415, 3418, 3481, 3766, 3817, 3927, 4723, 5387, 9677, 16941, 17088, 17917, 18046, 19600, 19937, 20214, 20678, 21002, 21382, 21701, 22245, 22327, 22558, 23209, 23318, 23605, 23770, 24222, 24782, 27797, 28958, 28973, 29256, 31656, 31923, 33816, 34585, 35565, 35737, 36960, 39710, 40411, 40520, 42679, 42991, 43830, 43848, 44497, 45882, 46203, 47435, 48387, 48617, 49312, 49962, 49986, 50414, 51603, 51945, 53977, 55495, 56166, 56898, 56955, 57177, 58315, 58534, 58882, 60287, 67235, 67854, 69933, 70129, 70617, 75302, 76912, 78077, 78426, 80160, 81165, 81432, 82569, 82730, 84897, 85474, 85881, 86243, 87005, 94914, 95349, 99992, etc.

The intrinsic factors matter. For example, the primitive part of $2^{147} - 1$ has the intrinsic factor 7 and one large prime factor. The $k$ for $b^k + 1$ are the $k = m/2$ for each even $m$ in the list above for $b^m - 1$. The list of $k$ begins 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 15, 16, 17, 19, 20, 21, 23, 27, 28, 31. With three exceptions, these $k$ are either odd or divisible by 4 because of the Aurifeuillian factorization

of $2^{4j-2}+1$. The exceptions are $2^2+1=5$, where the other Aurifeuillian factor is 1, $2^6+1=5\cdot 13$, where the 5 is an algebraic factor of one Aurifeuillian factor, and $2^{10}+1=5\cdot 5\cdot 41$, where the first 5 is algebraic and the second 5 is intrinsic. See Brillhart et al. [4] for details. For all larger $k\equiv 2 \pmod 4$, both Aurifeuillian factors are $>1$, so the primitive part is composite.

The lists for $F_m$ and $L_m$ are shorter because they show only $m$ for which the primitive part, with intrinsic factors removed, is $\equiv \pm 2 \pmod 5$. They omit, for example, $m=5$, 10, 11, 14, etc. The list of $m$ for $F_m$ are 3, 4, 7, 8, 9, 13, 16, 17, 23, 24, 32, 36, 43, 47, 48, 56, 83, 108, 137, 153, 192, 433, 972, 1431, 1892, 4723, 5387, 9677, 30757, 50833, 201107, etc. The $k$ for $L_k$ are the $k=m/2$ for each even $m$ in the list above for $F_m$. The list of $k$ begins 2, 4, 8, 12, 16, 18, 24, 28, 54, 96, etc. No $k$ in this list is a multiple of 5 because the primitive factors of $L_{5k}$ are all $\equiv 1 \pmod 5$ (see Proposition 2.10 of [6]) and we only looked at primitive parts $\equiv \pm 2 \pmod 5$.

## References


[1] R. Baillie, A. Fiori, and S. S. Wagstaff, Jr., Strengthening the Baillie-PSW primality test, *Math. Comp.*, **90** (2021), 1931–1955.

[2] R. Baillie and S. S. Wagstaff, Jr., Lucas Pseudoprimes, *Math. Comp.*, **35** (1980), 1391–1417.

[3] J. Brillhart, D. H. Lehmer, and J. L. Selfridge, New primality criteria and factorizations of $2^m \pm 1$, *Math. Comp.*, **29** (1975), 620–647.

[4] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, and S. S. Wagstaff, Jr, *Factorizations of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to High Powers*, Second edition, American Mathematical Society, Providence, RI, 1988.

[5] J. Feitsma, *Pseudoprimes*. Feitsma's web page is `http://www.janfeitsma.nl/math/psp2/index`. Statistics on psp(2) are at `http://www.janfeitsma.nl/math/psp2/statistics`. The database of all psp(2) $< 2^{64}$ is at `http://www.cecm.sfu.ca/Pseudoprimes/index-2-to-64.html`.

[6] J. Greene, J. Lim, S. Mashalkar, and E. F. Schaefer, Using Fibonacci factors to create Fibonacci pseudoprimes, *Fibonacci Quart.* **60**, (2022), 320—324.

[7] C. Pomerance, Are there counterexamples to the Baillie-PSW primality test?, in H. W. Lenstra, Jr., J. K. Lenstra, and P. Van Emde Boas, editors, *Dopo le parole angeboden aan Dr. A. K. Lenstra*. Amsterdam, 1984.

[8] C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr., The pseudoprimes to $25\cdot 10^9$, *Math. Comp.*, **35**, (1980), 1003–1026.

[9] A. Shallue and J. Webster, Algorithms for Carmichael numbers, preprint, `arXiv.org/abs/2506.09903v3`. The list of Carmichael numbers below $10^{24}$ is at `https://blue.butler.edu/~jewebste/`.

[10] S. S. Wagstaff, Jr. *The Joy of Factoring*, Student Mathematical Library, 68. American Mathematical Society, Providence, RI, 2013.

[11] H. C. Williams, *Édouard Lucas and Primality Testing*, Wiley, New York, 1998.