Better Bounds on the Rate of Non-Witnesses of Lucas Pseudoprimes

David Amirault

Mentor David Corwin

Project suggested by Stefan Wehmeier

Abstract

Efficient primality testing is fundamental to modern cryptography for the purpose of key generation. Different primality tests may be compared using their runtimes and rates of non-witnesses. With the Lucas primality test, we analyze the frequency of Lucas pseudoprimes using MATLAB. We prove that a composite integer n can be a strong Lucas pseudoprime to at most $\frac{1}{6}$ of parameters P, Q unless n belongs to a short list of exception cases, thus improving the bound from the previous result of $\frac{4}{15}$. We also explore the properties obeyed by such exceptions and how these cases may be handled by an extended version of the Lucas primality test.

1 Introduction

With the advent of public-key cryptosystems in the 1970s, the demand for faster primality tests has increased dramatically, leading to the discovery and rise in popularity of such probabilistic algorithms as the Miller-Rabin, Lucas, and Frobenius primality tests. Given the growing demand for large prime numbers in the field of cryptography, even modest improvements to current algorithms may lead to increased levels of internet security. As such, taking steps to understand more about primality tests and their rates of non-witnesses has vast applications in modern society. We now examine the Lucas primality test and its distribution of pseudoprimes with respect to their prime factorizations.

For P and Q fixed integers, we consider the Lucas sequences U and V defined by the recurrence relations:

$$\begin{cases} U_0 = 0, \qquad U_1 = 1, \qquad U_{k+2} = PU_{k+1} - QU_k, \\ V_0 = 2, \qquad V_1 = P, \qquad V_{k+2} = PV_{k+1} - QV_k. \end{cases}$$

Let $D = P^2 - 4Q$ and $\varepsilon(n)$ represent the Jacobi symbol (D/n). The following is a well-known result from which the strong Lucas pseudoprime test may be derived [2]:

Theorem 1. *Let p be a prime number relatively prime to $2QD$. Put $p - \varepsilon(p) = 2^k q$ with q odd. One of the following is true:*

$$p \mid U_q$$

or

$$\text{there exists } i \text{ such that } 0 \leq i < k \text{ and } p \mid V_{2^i q},$$

where U, V are the Lucas sequences of the parameters P, Q.

A composite integer n satisfying the above conditions is known as a strong Lucas pseudoprime to parameters P and Q, or slpsp(P, Q), using the notation of Arnault [1].

Definition 1. The set of ordered pairs of non-witnesses (P, Q) is given by

$$SL(D, n) = \#\left\{ (P, Q) \,\middle|\, \begin{array}{ll} 0 \le P, Q < n, & P^2 - 4Q \equiv D \text{ modulo } n, \\ \gcd(Q, n) = 1, & n \text{ is slpsp}(P, Q). \end{array} \right\}$$

Definition 2. We define a function analogous to Euler's totient function: the φ_D function, whose value is equal to the order of the unit group of $(\mathcal{O}/n\mathcal{O})$, where $\mathcal{O}$ is the ring of integers of the quadratic field $\mathbb{Q}[\sqrt{D}]$. φ_D is defined as

$$\begin{cases} \varphi_D(p^r) = p^{r-1}(p - \varepsilon(p)) & \text{for any prime } p \nmid 2D, \text{ and } r \in \mathbb{N}^*, \\ \varphi_D(n_1 n_2) = \varphi_D(n_1)\varphi_D(n_2) & \text{for any } n_1 \text{ and } n_2 \text{ relatively prime.} \end{cases}$$

Let $p_1^{r_1} \dots p_s^{r_s}$ be the prime decomposition of an integer $n > 2$ relatively prime to $2D$. Put

$$\begin{cases} n - \varepsilon(n) = 2^k q, \\ p_i - \varepsilon(p_i) = 2^{k_i} q_i \quad \text{for } 1 \le i \le s, \end{cases} \qquad \text{with } q, q_i \text{ odd},$$

with the p_i's ordered such that $k_1 \le \ldots \le k_s$.

Theorem 2 (Arnault)**.** *The number of pairs (P, Q) with $0 \le P, Q \le n$, $\gcd(Q, n) = 1$, $P^2 - 4Q \equiv D$ modulo n and such that n is an* slpsp(P, Q) *is expressed by the following formula:*

$$SL(D, n) = \prod_{i=1}^{s}(\gcd(q, q_i) - 1) + \sum_{j=0}^{k_1 - 1} 2^{js} \prod_{i=1}^{s} \gcd(q, q_i). \tag{1}$$

In the Methods section below, we will briefly examine the process by which data was collected using MATLAB and present a sample data table. The Results section will focus on extending the above formula using the φ_D function and using it to improve the bound given by Arnault [1]. A short lemma at the beginning of the Results section precedes the main result, Theorem 3. The proof is divided into cases based on s-values, which range from 1 to 4. We conclude by examining possible follow-up problems in the Future Work section, including applications of Newton's Method and the Baillie-PSW primality test.

2 Methods

Throughout the process of collecting data on the distribution of Lucas pseudoprimes, over a dozen MATLAB programs were written. The integers less than some arbitrary bound (100000 was used) with the highest rates of non-witnesses were grouped based on their prime factorizations to aid with the process of generalizing to integers with different s-values. After numerous values of D corresponding to different quadratic integer rings were tested, patterns emerged in the prime factorizations of integers that were frequently Lucas pseudoprimes, leading to the main result given below. Alternate primality tests, including the Miller-Rabin and Baillie-PSW tests, were coded in MATLAB as well to be compared to the Lucas test.

Table 1: Example Integers with High Rates of Non-Witnesses for $D = 5$

Integer	Non-Witness Rate	1st Prime Factor	2nd Prime Factor	3rd Prime Factor
21	.2381	3	7	
323	.4489	17	19	
377	.2255	13	29	
901	.1609	17	53	
1081	.1785	23	47	
1891	.2226	31	61	
3827	.1842	43	89	
4181	.1638	37	113	
5671	.2478	53	107	
5777	.2432	53	109	
6601	.1659	7	23	41
10207	.1592	59	173	
10877	.2450	73	149	
11663	.3705	107	109	
13861	.1879	83	167	
14981	.1589	71	211	
17119	.2250	17	19	53
18407	.1611	79	233	
19043	.4928	137	139	
25651	.2489	113	227	
		$\vdots$		

Figure 1: n with Non-Witness Rate Exceeding 1/6 for $s = 2$

- $n = (k + 1) * (k - 1), \quad (D/k + 1) = 1, \quad (D/k - 1) = -1$ (twin primes case)
- $n = (2k - 1) * (4k - 1), \quad (D/2k - 1) = -1, \quad (D/4k - 1) = -1$
- $n = (2k + 1) * (4k + 1), \quad (D/2k + 1) = 1, \quad (D/4k + 1) = 1$
- $n = (2k - 1) * (4k + 1), \quad (D/2k - 1) = -1, \quad (D/4k + 1) = 1$
- $n = (2k + 1) * (4k - 1), \quad (D/2k + 1) = 1, \quad (D/4k - 1) = -1$

Figure 2: n with Non-Witness Rate Exceeding 1/6 for $s = 3$

- $665 = (6 - 1)(6 + 1)(18 + 1), \quad q = 3^2 \cdot 37$
- $3655 = (6 - 1)(18 - 1)(42 + 1), \quad q = 3^2 \cdot 7 \cdot 29$
- $17119 = (18 - 1)(18 + 1)(54 - 1), \quad q = 3^3 \cdot 317$
- $20705 = (6 - 1)(42 - 1)(102 - 1), \quad q = 3^1 \cdot 7 \cdot 17 \cdot 29$
- $39689 = (14 - 1)(42 + 1)(70 + 1), \quad q = 3^4 \cdot 5 \cdot 7^2$
- $76589 = (18 + 1)(30 - 1)(138 + 1), \quad q = 3^2 \cdot 5 \cdot 23 \cdot 37$

3 Results

Lemma 1.

$$\frac{SL(D,n)}{\varphi_D(n)} = \frac{1}{2^{k_1+\ldots+k_s}} \cdot \prod_{i=1}^{s} \frac{1}{p_i^{r_i-1}} \cdot \left(\prod_{i=1}^{s} \frac{\gcd(q,q_i)-1}{q_i} + \frac{2^{sk_1}-1}{2^s-1} \cdot \prod_{i=1}^{s} \frac{\gcd(q,q_i)}{q_i} \right) \quad (2)$$

Proof. From Definition 2, we have that

$$\varphi_D(n) = \prod_{i=1}^{s} \varphi_D(p_i^{r_i}) = \prod_{i=1}^{s} p_i^{r_i-1}(2^{k_i}q_i) = 2^{k_1+\ldots+k_s} \cdot \prod_{i=1}^{s} q_i \cdot \prod_{i=1}^{s} p_i^{r_i-1} \quad (3)$$

Combining (1) and (3) and expanding the geometric series yields the desired expression.

□

Theorem 3. $SL(D,n) \le \frac{1}{6}n$ *unless one of the following is true:*

$$n = 9 \text{ or } 25$$

$$n = (2^{k_1}q_1 - 1)(2^{k_1}q_1 + 1)$$

$$n = (2^{k_1}q_1 + \varepsilon_1)(2^{k_1+1}q_1 + \varepsilon_2)$$

$$n = (2^{k_1}q_1 + \varepsilon_1)(2^{k_1}q_2 + \varepsilon_2)(2^{k_1}q_3 + \varepsilon_3), \quad q_1, q_2, q_3 \mid q,$$

where ε_i *means* $\varepsilon(p_i)$.

Proof. For the sake of completeness, we start with the case $s = 1$, although such n do not pose a significant problem to primality tests (perfect nth powers may be quickly detected using Newton's method).

$s = 1$. We know that all of the product expressions in (2) are bounded above by 1. Thus, we have

$$\frac{SL(D,n)}{\varphi_D(n)} \le \frac{1}{2^{k_1}} \cdot \prod_{i=1}^{s} \frac{1}{p_i^{r_i-1}}(1 + 2^{k_1} - 1) = \frac{1}{p_1^{r_1-1}}.$$

If $p_1 \ge 7$, then $\varphi_D(n) \le \frac{8}{7}n$ by definition. But $r_1 \ge 2$ because n is composite, so $SL(D,n) \le \frac{8}{49}n < \frac{1}{6}n$. Thus $n = 9$ or 25 in this case.

$s = 2$. Suppose $r_h \ne 1$ for some h.

- $q_h = 1$.

  We know that gcd$(q, q_h) = 1$ and $\prod_{i=1}^{s} \frac{\gcd(q,q_i)-1}{q_i} = 0$. Therefore, (2) reduces to

  $$\frac{SL(D,n)}{\varphi_D(n)} \le \frac{1}{4^{k_1}} \cdot \prod_{i=1}^{2} \frac{1}{p_i^{r_i-1}} \cdot \frac{4^{k_1}-1}{3}.$$

  If $k_h \le 2$, then $SL(D,n) \le \frac{1}{16} \cdot \frac{1}{3} \cdot \frac{15}{3} \cdot \varphi_D(n) \le \frac{5}{48} \cdot \frac{4}{3} \cdot \frac{6}{5}n = \frac{1}{6}n$ by the definition of $\varphi_D(n)$.

  If $k_h \ge 3$, then $SL(D,n) \le \frac{1}{4^{k_1}} \cdot \frac{1}{7} \cdot \frac{4^{k_1}}{3} \cdot \varphi_D(n) \le \frac{1}{21} \cdot \frac{4}{3} \cdot \frac{6}{5}n < \frac{1}{6}n$ because p_h is at least $2^{k_h}q_h - 1 \ge 7$.

- $q_h \ne 1$.

  Instead, (2) gives

  $$\frac{SL(D,n)}{\varphi_D(n)} \le \frac{1}{4^{k_1}} \cdot \prod_{i=1}^{2} \frac{1}{p_i^{r_i-1}} \cdot \left(1 + \frac{4^{k_1}-1}{3}\right).$$

  If $k_h = 1$, then $SL(D,n) \le \frac{1}{4} \cdot \frac{1}{5} \cdot (1+1) \cdot \varphi_D(n) \le \frac{1}{10} \cdot \frac{4}{3} \cdot \frac{6}{5}n < \frac{1}{6}n$.

  If $k_h \ge 2$, then $SL(D,n) \le \frac{1}{11} \cdot \left(\frac{1}{16} + \frac{1}{3}\right) \cdot \varphi_D(n) < \frac{1}{6}n$ because p_h is at least

$2^{k_h} q_h - 1 \geq 11$.

So $r_1 = r_2 = 1$ and $n = p_1 p_2 = \left(2^{k_1} q_1 + \varepsilon_1\right)\left(2^{k_2} q_2 + \varepsilon_2\right) = 2^{k_1+k_2} q_1 q_2 + 2^{k_1} q_1 \varepsilon_2 + 2^{k_2} q_2 \varepsilon_1 + \varepsilon_1 \varepsilon_2$. Therefore $n - \varepsilon_1\varepsilon_2 = n - \varepsilon(n) = 2^{k_1+k_2} q_1 q_2 + 2^{k_1} q_1 \varepsilon_2 + 2^{k_2} q_2 \varepsilon_1$. But $n - \varepsilon(n) = 2^k q$, so if $\gcd(q, q_1) = q_1$, then $q_1 \mid q \mid (n - \varepsilon(n))$ and $q_1 \mid q_2$. Also, if $\gcd(q, q_2) = q_2$, then $q_2 \mid q_1$. Suppose $q_1 \neq q_2$.

- If $\gcd(q, q_j) = 1$ for some j, then our lemma states that

$$\frac{SL(D,n)}{\varphi_D(n)} \leq \frac{4^{k_1} - 1}{3 \cdot 4^{k_1}} \cdot \prod_{i=1}^{2} \frac{\gcd(q, q_i)}{q_i}.$$

  If $q_j \neq 1$ and $k_j = 1$, then $SL(D,n) \leq \frac{1}{4} \cdot \frac{1}{3} \cdot \varphi_D(n) \leq \frac{1}{12} \cdot \frac{4}{3} \cdot \frac{6}{5} n < \frac{1}{6} n$.
  If $q_j \neq 1$ and $k_j \geq 2$, then $SL(D,n) \leq \frac{1}{3} \cdot \frac{1}{3} \cdot \varphi_D(n) \leq \frac{1}{9} \cdot \frac{12}{11} \cdot \frac{4}{3} n < \frac{1}{6} n$ because p_j is at least $2^{k_j} q_j - 1 \geq 11$.
  Now consider the case where $q_j = 1$. Let the other q be called q_ℓ. Then $\gcd(q, q_\ell) = q_\ell \implies q_\ell \mid q_j \implies q_\ell = q_j$, a contradiction, so $\gcd(q, q_\ell) \neq q_\ell$ and $\frac{\gcd(q, q_\ell)}{q_\ell} \leq \frac{1}{3}$.
  If $k_j = 1$, then $SL(D,n) \leq \frac{1}{4} \cdot \frac{1}{3} \cdot \varphi_D(n) \leq \frac{1}{12} \cdot \frac{4}{3} \cdot \frac{6}{5} n < \frac{1}{6} n$.
  If $k_j \geq 2$, then $SL(D,n) \leq \frac{1}{3} \cdot \frac{1}{3} \cdot \varphi_D(n) \leq \frac{1}{9} \cdot \frac{12}{11} \cdot \frac{4}{3} n < \frac{1}{6} n$.

- If $\gcd(q, q_j) \neq 1$ for both j, then we know

$$\frac{SL(D,n)}{\varphi_D(n)} \leq \frac{1}{2^{k_1+k_2}} \cdot \left[\prod_{i=1}^{2} \frac{\gcd(q, q_i) - 1}{q_i} + \frac{4^{k_1} - 1}{3} \cdot \prod_{i=1}^{2} \frac{\gcd(q, q_i)}{q_i}\right].$$

  It is true that $\gcd(q, q_1) \neq q_1$ or $\gcd(q, q_2) \neq q_2$ because if both were equal, then q_1 would equal q_2, a contradiction. Thus $\prod_{i=1}^{2} \frac{\gcd(q, q_i)}{q_i} \leq \frac{1}{3}$.
  If $k_2 - k_1 \geq 1$, then $SL(D,n) \leq \left[\frac{1}{8} \cdot \frac{1}{3} + \frac{1}{6} \cdot \frac{1}{3}\right] \cdot \varphi_D(n) \leq \frac{7}{72} \cdot \frac{4}{3} \cdot \frac{6}{5} n < \frac{1}{6} n$,

so $k_1 = k_2$. Arnault showed that the upper bound given above for $\frac{SL(D,N)}{\varphi_D(n)}$ is a decreasing function of k_1, so we expand the product at $k_1 = 1$:

$$\frac{SL(D,n)}{\varphi_D(n)} \leq \frac{1}{4} \cdot \left[2 \cdot \prod_{i=1}^{2} \frac{\gcd(q,q_i)}{q_i} - \frac{\gcd(q,q_1)}{q_1 q_2} - \frac{\gcd(q,q_2)}{q_1 q_2} + \frac{1}{q_1 q_2} \right].$$

We know that $\varphi_D(n) = 4^{k_1} q_1 q_2$, so $SL(D,n) \leq 2 \cdot \gcd(q,q_1) \cdot \gcd(q,q_2) - \gcd(q,q_1) - \gcd(q,q_2) + 1$. In the case of maximal $\varphi_D(n)$ when $\varepsilon_1 = \varepsilon_2 = -1$, we have $n = (2q_1 - 1)(2q_2 - 1)$. Without loss of generality, suppose q_1 is the q_j for which $\frac{\gcd(q,q_j)}{q_j} \leq \frac{1}{3}$. Hence

$$\frac{SL(D,n)}{n} \leq \frac{2 \cdot q_1/3 \cdot q_2 - q_1/3 - q_2 + 1}{(2q_1-1)(2q_2-1)} = \frac{(2q_1-1)(2q_2-1) - (4q_2 - 5)}{6(2q_1-1)(2q_2-1)} < \frac{1}{6}.$$

because $\gcd(q,q_2) \neq 1 \implies q_2 \neq 1$.

Finally, (2) tells us

$$\frac{SL(D,n)}{\varphi_D(n)} \leq \frac{1}{2^{k_1+k_2}} \cdot \frac{4^{k_1} - 1}{3}.$$

If $k_2 - k_1 \geq 2$, then

$$\frac{SL(D,n)}{\varphi_D(n)} \leq \frac{1}{4^{k_1} \cdot 4} \cdot \frac{4^{k_1}}{3}$$

and $SL(D,n) \leq \frac{1}{12} \cdot \varphi_D(n) \leq \frac{1}{12} \cdot \frac{4}{3} \cdot \frac{6}{5} n < \frac{1}{6} n$. We have shown that $r_1 = r_2 = 1$, $k_2 - k_1 = 0$ or 1, and $q_1 = q_2$. Thus, in the case of $s = 2$, the only remaining cases are $n = (2^{k_1} q_1 - 1)(2^{k_1} q_1 + 1)$ and $n = (2^{k_1} q_1 + \varepsilon_1)(2^{k_1+1} q_1 + \varepsilon_2)$.

$s = 3$. If there exists r_j with $r_j \neq 1$, then $\frac{SL(D,n)}{\varphi_D(n)} \leq \frac{1}{8} \cdot \frac{1}{3} \cdot (1+1) = \frac{1}{12}$. Likewise, if there exists q_j with $\gcd(q,q_j) \neq q_j$, then $\frac{SL(D,n)}{\varphi_D(n)} \leq \frac{1}{8} \cdot \left(\frac{1}{3} + \frac{1}{3}\right) = \frac{1}{12}$. In either case,

$SL(D,n) \leq \frac{1}{12} \cdot \varphi_D(n) \leq \frac{1}{12} \cdot \frac{4}{3} \cdot \frac{6}{5} \cdot \frac{8}{7} n < \frac{1}{6} n.$

Going back to our lemma, we have

$$\frac{SL(D,n)}{\varphi_D(n)} \leq \frac{1}{2^{k_1+k_2+k_3}} \cdot \left(\prod_{i=1}^{3} \frac{\text{gcd}(q,q_i)-1}{q_i} + \frac{8^{k_1}-1}{7} \right).$$

Suppose that $k_1 \neq k_3$.

- If $q_j = 1$ for some j, then $SL(D,n) \leq \frac{1}{16} \cdot \frac{8}{7} \cdot \varphi_D(n) \leq \frac{1}{14} \cdot \frac{4}{3} \cdot \frac{6}{5} \cdot \frac{8}{7} n < \frac{1}{6} n.$
- Otherwise, if the least q_j is equal to 3, then $SL(D,n) \leq \frac{1}{16} \cdot \left(\frac{2}{3}+1\right) \cdot \varphi_D(n) \leq \frac{1}{16} \cdot \frac{5}{3} \cdot \frac{6}{5} \cdot \frac{8}{7} \cdot \frac{12}{11} n < \frac{1}{6} n$ because the least possible value for p_j is $2^1 \cdot 3 - 1 = 5$.
- Lastly, $SL(D,n) \leq \frac{1}{16} \cdot (1+1) \cdot \varphi_D(n) \leq \frac{1}{8} \cdot \frac{12}{11} \cdot \frac{14}{13} \cdot \frac{18}{17} n < \frac{1}{6} n.$

So $k_1 = k_2 = k_3$ and $n = (2^{k_1} q_1 + \varepsilon_1)(2^{k_1} q_2 + \varepsilon_2)(2^{k_1} q_3 + \varepsilon_3)$ with $q_1, q_2, q_3 \mid q$.

$s \geq 4$. We start with

$$\frac{SL(D,n)}{\varphi_D(n)} \leq \frac{1}{2^{k_1+\ldots+k_4}} \cdot \left(\prod_{i=1}^{4} \frac{\text{gcd}(q,q_i)-1}{q_i} + \frac{16^{k_1}-1}{15} \right).$$

- If some $q_j = 1$, then $SL(D,n) \leq \frac{1}{16} \cdot \frac{16}{15} \cdot \varphi_D(n) \leq \frac{1}{15} \cdot \frac{4}{3} \cdot \frac{6}{5} \cdot \frac{8}{7} \cdot \frac{12}{11} n < \frac{1}{6} n.$
- When the two least q values are both 3, $SL(D,n) \leq \frac{1}{16} \cdot \left(\frac{2}{3} \cdot \frac{2}{3}+1\right) \cdot \varphi_D(n) \leq \frac{1}{16} \cdot \frac{13}{9} \cdot \frac{6}{5} \cdot \frac{8}{7} \cdot \frac{12}{11} \cdot \frac{14}{13} n < \frac{1}{6} n.$
- When the least q value is 3 but the second least q value is greater than 3, we know $SL(D,n) \leq \frac{1}{16} \cdot \left(\frac{2}{3}+1\right) \cdot \varphi_D(n) \leq \frac{1}{16} \cdot \frac{5}{3} \cdot \frac{6}{5} \cdot \frac{12}{11} \cdot \frac{14}{13} \cdot \frac{18}{17} n < \frac{1}{6} n.$
- Otherwise, $SL(D,n) \leq \frac{1}{16} \cdot (1+1) \cdot \varphi_D(n) \leq \frac{1}{8} \cdot \frac{12}{11} \cdot \frac{14}{13} \cdot \frac{18}{17} \cdot \frac{20}{19} n < \frac{1}{6} n.$

Therefore, if $s = 4$, then $SL(D, n) < \frac{1}{6}$. $\square$

4 Future Work

The exceptions for $s = 2$ may be handled using Newton's Method for approximating the roots of real functions; there are only 5 such problem cases to consider. However, when $s = 3$, the number of exceptions to the $\frac{1}{6}n$ bound are too numerous to be determined with Newton's Method. Fortunately, in all cases except for the famous Carmichael numbers, those composite numbers with three or more prime factors tend to have low rates of non-witnesses when examined with the related Miller-Rabin primality test [5].

The complementary nature of the Miller-Rabin primality test and the strong Lucas test is exploited by the Baillie-PSW primality test, which combines a Miller-Rabin test using the parameter $a = 2$ with a strong Lucas test. No known composites pass this test, although probabilistic results suggest that counterexamples do exist [3, 4]. It would be interesting to determine specific properties that must be obeyed by all Baillie-PSW pseudoprimes. Such results would also be applicable in the field of cryptography as the Baillie-PSW primality test is very widely used; the apparent lack of non-witnesses makes the test more reliable than the bounds on the Miller-Rabin and Lucas tests would suggest.

5 Acknowledgements

First and foremost, I would like to thank my mentor David Corwin for his guidance throughout the research process. Also, I would like to recognize Dr. Stefan Wehmeier from MathWorks for suggesting the project. This research would not have been possible without the MIT PRIMES faculty, especially head mentor Dr. Tanya Khovanova, Chief Research Advisor Dr. Pavel Etingof, and Program Director Dr. Slava Gerovitch.

References

[1] F. Arnault, *The rabin-monier theorem for lucas pseudoprimes*, Math. Comp. (1997), 869–881.

[2] Robert Baillie and Jr. Samuel S. Wagstaff, *Lucas pseudoprimes*, Math. Comp. (1980), 1391–1417.

[3] Zhuo Chen and John Greene, *Some comments on baillie-psw pseudoprimes*, Fibonacci Quarterly (2003), 334–344.

[4] Carl Pomerance, *Are there counter-examples to the baillie-psw primality test?*, (1984).

[5] Michael O. Rabin, *Probabilistic algorithm for testing primality*, J. Number Theory (1980), 128–138.