STRENGTHENING THE BAILLIE-PSW PRIMALITY TEST

ROBERT BAILLIE, ANDREW FIORI, AND SAMUEL S. WAGSTAFF, JR.

Abstract. In 1980, the first and third authors proposed a probabilistic primality test that has become known as the Baillie-PSW (BPSW) primality test. Its power to distinguish between primes and composites comes from combining a Fermat probable prime test with a Lucas probable prime test. No odd composite integers have been reported to pass this combination of primality tests if the parameters are chosen in an appropriate way. Here, we describe a significant strengthening of this test that comes at almost no additional computational cost. This is achieved by including in the test Lucas-V pseudoprimes, of which there are only five less than 10^{15}.

1. Introduction

A (Fermat) *base-a pseudoprime*, or psp(a), is a composite positive integer n that satisfies the conclusion of Fermat's little theorem, that is

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

For each integer base $a > 1$, there are infinitely many pseudoprimes, but they are sparser than primes. In [5], the first and third authors studied analogues of pseudoprimes in which $a^{n-1} - 1$ is replaced by a Lucas sequence.

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 P and Q are defined for $k \geq 2$ by

$$U_k = PU_{k-1} - QU_{k-2} \quad \text{and} \quad V_k = PV_{k-1} - QV_{k-2}.$$

Let $n > 1$ be an odd positive integer. Choose D, P, and Q so that the Jacobi symbol $(D/n) = -1$. It is well known [5], [8] that if n is prime and $(n, Q) = 1$, then

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

$$V_{n+1} \equiv 2Q \pmod{n}. \tag{2}$$

In [5], we defined a *Lucas pseudoprime* with parameters P and Q to be a *composite* integer n satisfying (1). We proposed a fast probable prime test by combining the Lucas primality criterion in (1) with a (Fermat) probable prime test.

In this paper, we emphasize the importance of the primality criterion in Congruence (2). We found that, using a standard method of choosing D, P, and Q, among the composite n under 10^{15}, there are over two million that satisfy (1), but only *five* that satisfy (2).

2010 *Mathematics Subject Classification.* Primary 11Y11; Secondary 11A51.

Key words and phrases. primality test, Lucas sequences.

A.F.'s work was supported partially by the University of Lethbridge and NSERC.

S.S.W.'s work was supported by the CERIAS Center at Purdue University.

Layout of this paper.

- Section 2: we give details on Fermat and Lucas pseudoprimes and describe how to efficiently compute terms in the Lucas sequences;
- Section 3: we define the original Baillie-PSW primality test, we list applications that use this test, and we summarize calculations that have been performed over the past 40 years;
- Section 4: we summarize the data on pseudoprimes up to 10^{15};
- Section 5: we discuss whether the scarcity of composite solutions to (2) is due to the particular method for choosing P and Q;
- Section 6: we propose a strengthened primality test that includes Congruence (2) and offer a reward for a counterexample;
- Section 7: discusses the importance of choosing Q to be neither $+1$ nor $-1 \pmod n$;
- Section 8: we reprise Pomerance's heuristic argument that there are infinitely many counterexamples to the enhanced test;
- Appendix A: we prove that two popular methods for choosing P and Q produce exactly the same Lucas pseudoprimes.

The authors thank Carl Pomerance for suggesting the proof of Theorem 2 in Section 8.

2. Background

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

$$a^{n-1} \equiv 1 \pmod n. \tag{3}$$

The converse of Fermat's little theorem is not true, but if (3) is true for a given $a > 1$, then n is likely to be prime.

A *base-a pseudoprime*, or psp(a), is a *composite* n that satisfies (3).

Base-2 pseudoprimes up to $25 \cdot 10^9$ were studied in detail in [22]. The first ten base-2 pseudoprimes are 341, 561, 645, 1105, 1387, 1729, 1905, 2047, 2465, and 2701.

Since [22] appeared in 1980, Feitsma [11] has computed the psp(2) $< 2^{64} \approx 1.8 \cdot 10^{19}$. There are 118 968 378 of them.

There are $\pi(2^{64}) - 1 = 425\,656\,284\,035\,217\,742$ odd primes $< 2^{64}$ [25]. Therefore, up to 2^{64}, congruence (3) with $a = 2$ holds for $425\,656\,284\,035\,217\,742 + 118\,968\,378$ values of n, of which 99.9999999721 percent are prime. This is why, if $2^{n-1} \equiv 1 \pmod n$, it is legitimate to call n a *probable prime*, and why this congruence is sometimes used as part of a test for primality.

Euler's criterion states that if n is an odd prime and $(a, n) = 1$, then

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod n, \tag{4}$$

where $\left(\frac{a}{n}\right)$ is the Jacobi symbol. A composite number that satisfies this congruence is called a *base-a Euler pseudoprime* (epsp(a)). The first ten epsp(2) are 561, 1105, 1729, 1905, 2047, 2465, 3277, 4033, 4681, and 6601. The epsp(a) are a proper subset of the psp(a). About half of the psp(a) are epsp(a) [22, p. 1005], so (4) is a slightly stronger primality test than (3).

2.2. **Strong probable primes and pseudoprimes.** We now describe an even stronger, and more widely-used primality test, also based on Fermat's little theorem. [22] defines *strong* probable primes and *strong* pseudoprimes. 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

$$a^d \equiv 1 \pmod n, \quad \text{or} \tag{5}$$

$$a^{d \cdot 2^r} \equiv -1 \pmod n, \quad \text{for some } r \text{ with } 0 \le r < s. \tag{6}$$

If either (5) or (6) is true, then n is called a *base-a strong probable prime* (sprp(a)). If either of these holds, then we also have $a^{n-1} = a^{d \cdot 2^s} \equiv 1 \pmod{n}$.

If n is composite and either (5) or (6) is true, then n is called a *base-a strong pseudoprime* (spsp(a)). The spsp(a) are a proper subset of psp(a), and so are scarcer than psp(a). For example, of the 118 968 378 psp(2) $< 2^{64}$ found by Feitsma, only 31 894 014 are spsp(2) [11]. The first ten base-2 strong pseudoprimes are 2047, 3277, 4033, 4681, 8321, 15841, 29341, 42799, 49141, and 52633.

The spsp(a) are also a proper subset of epsp(a). Therefore, it makes sense for a primality test to use the strong conditions (5) and (6) instead of (3) or (4).

To efficiently compute a^{n-1}, we use the binary expansion of $n-1$. The number of steps is essentially the number of *binary digits* in n, that is, $\log_2(n)$. All of the calculations are performed modulo n to keep the sizes of the numbers reasonable. Details and a worked example can be found in the preprint of this article, [6].

A *Carmichael number* is a composite integer n that is a pseudoprime to every base a for which $(a, n) = 1$. They are also sparse, although there are infinitely many of them [2]. However, there are no *strong* Carmichael numbers, that is, there is no composite n which is *strong* pseudoprime to all bases relatively prime to n: Rabin proved [23, Theorem 1] that any composite n is a strong pseudoprime to at most 1/4 of bases a, $1 \le a < n$.

2.3. **Lucas sequences and pseudoprimes; Lucas-V pseudoprimes.** Lucas sequences, and their applications to prime-testing, were discussed in [5] and [8].

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 P and Q are defined recursively for $k \ge 2$ by

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

For $k \ge 0$ we also have

$$U_k = (\alpha^k - \beta^k)/(\alpha - \beta) \quad \text{and} \quad V_k = \alpha^k + \beta^k\,,$$

where α and β are the distinct roots of $x^2 - Px + Q = 0$. Note that $\alpha\beta = Q$ and $\alpha + \beta = P$.

When n is an odd positive integer, write $\delta(n) = n - (D/n)$ where (D/n) is the Jacobi symbol. It is known [5, pp. 1391-1392], [8, Theorem 8] that if n is prime and $(n, Q) = 1$, then

$$U_{\delta(n)} \equiv 0 \pmod{n}, \tag{7}$$

$$V_{\delta(n)} \equiv 2Q^{(1-(D/n))/2} \pmod{n}, \quad \text{provided} \quad (n, D) = 1, \tag{8}$$

$$U_n \equiv (D/n) \pmod{n}, \tag{9}$$

$$V_n \equiv V_1 = P \pmod{n}. \tag{10}$$

If $(n, 2PQD) = 1$, any two of these congruences imply the other two.

Lucas pseudoprimes were defined in [5]. These are analogues of Fermat pseudoprimes in which $a^{n-1} - 1$ is replaced by a Lucas sequence.

For reasons discussed in that paper, to use Lucas sequences for primality testing, we choose an algorithm for picking D, P, and Q based on n, and we require that the Jacobi symbol $(D/n) = -1$. If n is prime, $(n, D) = (n, Q) = 1$, and $(D/n) = -1$, then $\delta(n) = n + 1$ and congruences (7) and (8) become (1) and (2). These two congruences are key parts of the primality test that we propose below.

We'll discuss (2) in detail later. The other congruences, (9) and (10), also hold if n is prime, but these congruences are not very useful in primality testing [5, Section 6]: most composite n that satisfy congruence (9) have small prime factors; many composite n that satisfy (10) are psp(2).

If n satisfies (1), then n is called a *Lucas probable prime* with parameters P and Q, written lprp(P, Q). If n satisfies (1) and we know it is composite, then we call n a *Lucas pseudoprime*, written lpsp(P, Q). If n fails (1), then n is composite.

For convenience, we also introduce the following

Definition [7, p. 266]. If n satisfies (2), we call n a *Lucas-V probable prime* (vprp). If n is composite and satisfies (2) with parameters P and Q, we call n a *Lucas-V pseudoprime* (vpsp(P, Q)).

What we call vpsp's are sometimes called *Dickson pseudoprimes of the second kind* [24].

The authors of [5] proved that there are infinitely many Lucas pseudoprimes, but that they are rare compared to the primes.

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 [22] and mentioned in [5], and which seems to be widely used in primality testing, is:

Method A: Let D be the first element of the sequence 5, -7, 9, -11, 13, -15, ... 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 A sets $Q = -1$ fairly often, namely, when $n \equiv \pm 3 \pmod{10}$.)

We remarked in [5] that more composite n satisfying any of (7)–(10) had $Q \equiv \pm 1$ than $Q \not\equiv \pm 1 \pmod{n}$. This observation led the authors to define the following preferred method to select parameters, which forces $Q \not\equiv \pm 1 \pmod{n}$:

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

Method A* leaves $D = P^2 - 4Q$ unchanged from Method A.

It turns out that the Lucas pseudoprimes generated by Methods A and A* are the same. The same is true for strong Lucas pseudoprimes (see Section 2.4). We prove this in Appendix A.

If D, P, and Q are chosen with Method A*, the first ten lpsp are: 323, 377, 1159, 1829, 3827, 5459, 5777, 9071, 9179, and 10877.

Calculations performed for this paper show that when Method A* is used, there are 2 402 549 lpsp less than 10^{15}.

2.4. **Strong Lucas probable primes and pseudoprimes.** [5] defines *strong* Lucas probable primes and *strong* Lucas pseudoprimes. If n is odd, then we can write $n + 1 = d \cdot 2^s$ where d is odd. If n is prime and $(D/n) = -1$, then we will have either

$$U_d \equiv 0 \pmod{n}, \quad \text{or} \tag{11}$$

$$V_{d \cdot 2^r} \equiv 0 \pmod{n}, \quad \text{for some } r \text{ with } 0 \le r < s. \tag{12}$$

If $(D/n) = -1$ and n satisfies (11) or (12), 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), that is, $U_{n+1} = U_{d \cdot 2^s} \equiv 0 \pmod{n}$.

If $(D/n) = -1$, n satisfies (11) or (12) and is *composite*, then n is called a *strong Lucas pseudoprime*, written slpsp(P, Q).

If D, P, and Q are chosen with method A*, the first ten slpsp are: 5459, 5777, 10877, 16109, 18971, 22499, 24569, 25199, 40309, and 58519.

The slpsp(P, Q) are scarcer than lpsp(P, Q). For example, of the 2 402 549 lpsp less than 10^{15}, only 474971 are slpsp.

Because strong lpsp are rarer than lpsp, a sensible primality test will use the strong version of the Lucas test, Congruences (11) and (12), instead of (1).

The following equations show how to use the binary representation of $n+1$ to efficiently compute the values on the left sides of Congruences (11) and (12). We can also compute U_{n+1}, and, at almost

no added computational cost, V_{n+1} and Q^{n+1}.

$$U_{2k} = U_k V_k \tag{13}$$

$$V_{2k} = V_k^2 - 2Q^k \tag{14}$$

$$Q^{2k} = (Q^k)^2 \tag{15}$$

$$U_{k+1} = (PU_k + V_k)/2 \tag{16}$$

$$V_{k+1} = (DU_k + PV_k)/2 \tag{17}$$

$$Q^{k+1} = Q \cdot Q^k \tag{18}$$

Equations (13) and (14) are Equations 4.2.6 and 4.2.7 in Williams [28] while (16) and (17) are 4.2.21 in that book. Equations (13)–(15) are used to double the subscript and exponent; Equations (16)–(18) are used to increment the subscript and exponent. These equations are also given in [8, p. 628].

In Equations (16) and (17), if the numerator is odd, we increment it by n to make it be even. This is legitimate because n is odd, and we care only about the result modulo n.

A worked example with $n = 323$ is in the preprint of the present article, [6].

3. The original Baillie-PSW primality test

In [5], the first and third authors show that we get a very effective test for primality by combining Fermat and Lucas probable prime tests.

This combined test works so well because, in some sense, psp's and lpsp's tend to be different kinds of numbers. For example, the numbers that are psp(2) and those that are lpsp from Method A* tend to fall into residue classes $+1$ and -1, respectively, for small moduli [5, pp. 1404-1405]. A similar phenomenon is observed for psp(a) for other a, and for lpsp's generated by several other methods for choosing D, P, and Q.

The probable prime test we proposed in [5] has these steps:

(1) If n is not a strong base-2 probable prime, then n is composite, so stop.
(2) Choose Lucas parameters with Method A*. (If you encounter a D for which $(D/n) = 0$: if either $|D| < n$, or if $|D| \geq n$ but n does not divide $|D|$, then n is composite, so stop.)
(3) If n is not a strong Lucas probable prime with the chosen parameters, then n is composite. Otherwise, declare n to be (probably) prime.

If n is composite, the test almost always stops in the first step so the other steps are not needed. The test almost never stops in the second step. If n is prime, then all three steps are needed.

The authors of [22] and [5] observed that, up to $25 \cdot 10^9$, there was no overlap between the psp(2) and the lpsp from Method A*. Using more recent data from Feitsma [11], we find that none of the 118 968 378 psp(2) up to $2^{64} \approx 1.8 \cdot 10^{19}$ is an lpsp when Method A* is used. Therefore, this test correctly distinguishes primes from composites up to at least 2^{64}. Further, no one has reported a larger composite n that is both psp(2) and lpsp(P, Q) using method A*.

Richard Pinch [18], [19] has computed a list of all 20 138 200 Carmichael numbers up to 10^{21}. He kindly provided his list to the first author, for which we thank him. None of these Carmichael numbers is an lpsp when Method A* is used.

The reader might notice that the above test does not first check n for divisibility by small primes. This check is omitted because it is not necessary (although step 2 does sometimes find small factors). However, *for the sake of efficiency*, a practical primality test should first check to see whether n is divisible by small primes before proceeding to step 1.

Some version of this test is used as a fast algorithm for finding large probable primes in mathematical software packages like *FLINT*, *Maple*, *Mathematica*, *Pari/GP*, *SageMath*, and by programs for choosing large primes for public-key ciphers like RSA.

Several programming languages, like *GNU GMP*, *Java*, and *Perl* also provide functions for doing Fermat and Lucas tests.

While some cryptographic libraries use a combined Fermat/Lucas test, some do not. Albrecht, et al, were able to find composite numbers which some of the latter libraries declared were prime [1].

A reward of $620 was offered for an example of a composite n declared prime by this test. No one has claimed the reward after 40 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.

4. The data to 10^{15}

Recall that lpsp and vpsp are composite n that satisfy (1) and (2), respectively.

We computed the lpsp and vpsp up to 10^{15}, using Method A* to choose the Lucas parameters.

This calculation took about 750000 core-hours on the Rice cluster at Purdue University, plus about 10000 core-hours on computers at the University of Lethbridge.

The counts are shown in Table 1. What is striking is that, while there are about 2 million each of psp(2) and lpsp, there are only *five* vpsp.

These five numbers are shown in Table 2. For $n = 14\,760\,229\,232\,131$, Method A* set $P = 1$, $Q = 2$. For the other four n, Method A* set $P = Q = 5$.

Table 1. Number of psp(2), spsp(2), lpsp, slpsp, and vpsp with $n < 10^k$ using Method A*.

k	psp(2)	spsp(2)	lpsp	slpsp	vpsp
2	0	0	0	0	0
3	3	0	2	0	1
4	22	5	9	2	1
5	78	16	57	12	1
6	245	46	219	58	1
7	750	162	659	178	1
8	2057	488	1911	505	1
9	5597	1282	5485	1415	1
10	14884	3291	15352	3622	1
11	38975	8607	42505	9714	1
12	101629	22407	116928	25542	3
13	264239	58892	319687	67045	3
14	687007	156251	875270	178118	4
15	1801533	419489	2402549	474971	5

Table 2. vpsp $< 10^{15}$ using Method A*.

n	n factored	$n-1$ factored	$n+1$ factored
913	$11 \cdot 83$	$2^4 \cdot 3 \cdot 19$	$2 \cdot 457$
150 267 335 403	$3 \cdot 47 \cdot 89 \cdot 563 \cdot 21269$	$2 \cdot 157 \cdot 478\,558\,393$	$2^2 \cdot 1609 \cdot 23\,347\,939$
430 558 874 533	$75913 \cdot 5\,671\,741$	$2^2 \cdot 3^2 \cdot 11\,959\,968\,737$	$2 \cdot 197947 \cdot 1\,087\,561$
14 760 229 232 131	$2467 \cdot 5\,983\,068\,193$	$2 \cdot 3 \cdot 5 \cdot 107 \cdot 53569 \cdot$ $\cdot 85837$	$2^2 \cdot 3\,690\,057\,308\,033$
936 916 995 253 453	$2027 \cdot 21521 \cdot 21\,477\,559$	$2^2 \cdot 3 \cdot 37 \cdot 41 \cdot 1109 \cdot$ $\cdot 46\,409\,057$	$2 \cdot 389 \cdot 15313 \cdot$ $\cdot 78\,643\,211$

In Section 7, we give heuristic arguments as to why vpsp are so rare, especially when $Q \not\equiv \pm 1 \pmod{n}$.

When P and Q are chosen by Method A*, we found that (i) none of the five vpsp(P, Q) is an lpsp(P, Q), (ii) none of the 118 968 378 psp(2) less than 2^{64} is either an lpsp or a vpsp, and (iii) none

of the 20 138 200 Carmichael numbers below 10^{21} is either an lpsp or a vpsp. (We do not know if there is an $n > 10^{15}$ which is both lpsp(P, Q) and vpsp(P, Q).)

The enhanced primality test we propose in Section 6 is based on the rarity of vpsp, and on this absence of overlap between any two of spsp(2), slpsp, and vpsp.

Dana Jacobsen's website [15] displays counts of psp(2), spsp(2), lpsp, and slpsp less than 10^{15}, where P and Q are selected by method A (or A*), as well as other types of pseudoprimes. The lists of pseudoprimes can also be downloaded from that site.

5. Is there anything special about Method A*?

The reader may wonder whether the rarity of vpsp compared to lpsp is an artifact of using Method A* to choose D, P, and Q.

The answer appears to be "no", especially if we require that $Q \not\equiv \pm 1 \pmod{n}$. We compared several methods for choosing D, P, and Q; see Table 3.

For example, [5] describes Methods B and B*:

Method B: Let D be the first element of the sequence 5, 9, 13, 17, ... for which $(D/n) = -1$. Let P be the smallest odd number exceeding $\sqrt{D}$, and $Q = (P^2 - D)/4$.

Method B*: Choose D, P, and Q as in Method B. If $Q = 1$, replace Q by $P + Q + 1$ and replace P by $P + 2$ (this preserves the value of D).

For this paper, we also tested:

Method C: Same as Method A, except we start testing D's at $D = 41$ instead of at $D = 5$. This insures that Method C almost always produces a (P, Q) pair different from the pair produced by Method A.

Method D: Fix Q = 2. Try $P = 4, 5, 6, 7,$ ... until $(D/n) = -1$.

Method R1: Choose P and Q *at random* from a uniform distribution with $1 \le P, Q \le n - 1$, until $(D/n) = -1$. We used the *random( )* function in version 2.11.4 of *PARI/GP*, initialized with *PARI*'s default seed of 1.

Method R2: Same as Method R1, but initialized with the (randomly-selected) seed 737984.

We compared these eight methods for odd, composite $n < 10^{10}$.

Methods A*, B*, C, and D can never set $Q \equiv \pm 1 \pmod{n}$.

Method B yielded 5940 vpsp. Only one of these, $n = 64469$, occurred with $Q \not\equiv \pm 1 \pmod{n}$: This n is vpsp$(5, 3)$, but is not lpsp$(5, 3)$.

Method B* yielded two vpsp: $n = 913$ ($P = Q = 5$) and $n = 64469$ ($P = 5$, $Q = 3$).

No vpsp from Method R1 or R2 had $Q \equiv \pm 1 \pmod{n}$. This is not surprising: Q was a random integer between 1 and $n - 1$, and $Q \equiv \pm 1 \pmod{n}$ occurred for only eight n's with R1 and twelve with R2.

Method	lpsp	vpsp, $Q \equiv \pm 1$	vpsp, $Q \not\equiv \pm 1$	simultaneously lpsp and vpsp
A	15352	914	0	757
A*	15352	–	1	0
B	15019	5939	1	4374
B*	12879	–	2	0
C	13766	–	4	0
D	15957	–	6	0
R1	17065	0	3	0
R2	16863	0	4	0

Table 3. Number of lpsp and vpsp to 10^{10} using various methods for choosing P and Q.

All of the methods tested in Table 3 yielded fewer vpsp than lpsp. Moreover, if $Q \not\equiv \pm 1 \pmod{n}$, none of the lpsp$(P, Q)$ was also vpsp(P, Q). This Table supports the importance of choosing $Q \not\equiv \pm 1 \pmod{n}$.

6. The enhanced BPSW primality test

The enhanced primality test we propose here is based on the one described in Section 3. The most important strengthening is that we now include Congruence (2) to check whether n is a vprp. This has very little additional computational cost beyond the Lucas test in step 3.

The strong Lucas probable prime test, Congruences (11) and (12), allows us to stop the calculation one or more steps before reaching U_{n+1}, V_{n+1}, and $Q^{n+1} \pmod{n}$. Here, we assume that we continue the calculation for a few additional steps in order to obtain $Q^{(n+1)/2}$ and $V_{n+1} \pmod{n}$.

Here is our proposed enhanced primality test for odd, positive integer n:

(1) If n is not a strong probable prime to base 2, then n is composite; stop.
(2) Choose Lucas parameters with Method A*. If you encounter a D for which $(D/n) = 0$: if either $|D| < n$, or if $|D| \geq n$ but n does not divide $|D|$, then n is composite; stop.
(3) If n is not an slprp(P, Q), then n is composite; stop.
(4) If n is not a vprp(P, Q), then n is composite; stop.
(5) If n does not satisfy $Q^{(n+1)/2} \equiv Q \cdot (Q/n) \pmod{n}$, then n is composite; stop. Otherwise, declare n to be probably prime.

Recall that no composite number is known that passes steps 1 through 3. This test is more powerful than the original BPSW test because so few composite n satisfy step 4. A composite n that passes this test would have to be, simultaneously, spsp(2), slpsp(P, Q), *and* vpsp(P, Q). Consequently, we expect that a composite n would be even less likely to pass this test than to pass the original BPSW test.

An odd, composite n that is both an lpsp and a vpsp is a *Frobenius* pseudoprime [9, p. 145], [13], [14]. These are rare [15], in part because, as we've seen above, the vpsp are rare. Odd, composite n that pass this enhanced test should be even rarer.

Step 5 is a primality check based on Euler's criterion, Congruence (4). This is a relatively minor enhancement. However, since we essentially already have the power of Q necessary for the test, we may as well use it. Once we have calculated $Q^{(n+1)/2} = Q \cdot Q^{(n-1)/2} \pmod{n}$, we can compute (Q/n), then apply Euler's criterion to check whether

$$Q^{(n+1)/2} \equiv Q \cdot (Q/n) \pmod{n}.$$

If this congruence fails, then n is composite.

Suggestions for implementing this primality test.

1. For efficiency, before step 1, one should first check n for divisibility by small primes.

2. We recommend doing a (strong) Fermat test to base 2 instead of to some other base. As far as anyone knows, there is nothing inherently better about using base 2. However, because we know all psp(2) up to 2^{64}, we know that no psp(2) below that limit is an lpsp. We do not know whether this is true for other bases.

3. In step 2: If n happens to be a perfect square, then (D/n) will never be -1. So, after encountering, say, 20 D's with $(D/n) = 1$, one should check whether n is a perfect square; if so, it is composite. This can be done quickly using Newton's method; see [5, p. 1401].

4. It is easy to show that, if n is sprp(a), then n is also sprp$(\pm(a^k))$ for $k \geq 1$. Therefore, if Method A* chooses a Q such that $|Q|$ is a power of 2, then, because n is known from step 1 to be sprp(2), the test in step 5 will not strengthen the test. For $n < 10^9$, this happens about 28 percent of the time ($D = -7$, $Q = 2$; $D = -15$, $Q = 4$; $D = 17$, $Q = -4$, etc).

5. To compute all three of U_{n+1}, V_{n+1}, and $Q^{n+1} \pmod{n}$ takes roughly three times as many multi-precision operations as it takes to compute $2^{n-1} \pmod{n}$. Therefore, this enhanced BPSW test takes about as long as doing Fermat tests to four different bases. However, as noted in [22, p.

1020], if n is psp to base a, then n is more likely than the average number of that size to also be psp to some other base b. In other words, there are diminishing returns in doing repeated Fermat tests. Therefore, it makes more sense to do one Fermat test followed by the Lucas tests in steps 3 and 4, than to perform Fermat tests to four (or more) different bases.

Reward for a counterexample or for a proof that there are none.

A counterexample to this enhanced test would be a positive, odd composite n which this test declares is probably prime. The first and third authors each offer U.S. $1000 for either the first counterexample to this enhanced test, or the first proof, published in a peer-reviewed journal, that there are none. A claim that n is a counterexample must be accompanied by a (P, Q) pair that came from Method A*, for which the test claims n is probably prime. The claim must also be accompanied by a proof that n is composite: either a (not necessarily prime) factor of n that is larger than 1 and less than n, or a base a with $2 < a < n - 1$ for which n is not a base-a strong probable prime, or a (P, Q) pair not from Method A* such that $D = P^2 - 4Q$ has Jacobi symbol $(D/n) = -1$, but for which n is not slpsp(P, Q), or is not vpsp(P, Q).

7. Some Heuristics for lpsps and vpsps

We note that both conditions of (7) and (8) are both congruences modulo n, and thus if p is any prime which divides n, then we obtain implied congruences modulo p. That is if

$$U_{\delta(n)} \equiv 0 \pmod{n}, \qquad \text{then} \qquad U_{\delta(n)} \equiv 0 \pmod{p}$$

and if

$$V_{\delta(n)} \equiv 2Q^{(1-(D/n))/2} \pmod{n}, \qquad \text{then} \qquad V_{\delta(n)} \equiv 2Q^{(1-(D/n))/2} \pmod{p}.$$

Moreover, if n were square free, we have that the conditions modulo p for all p dividing n would give sufficient conditions for the same congruences modulo n.

Now, suppose we write $n = py$, we can assess the probability that for example

$$V_{\delta(n)} \equiv 2Q^{(1-(D/n))/2} \pmod{p}$$

by considering the probability that, as we vary y among y with $(D/py) = (D/n)$,

$$V_{\delta(py)} \equiv 2Q^{(1-(D/py))/2} \pmod{p}.$$

We note that this quantity only depends on y modulo the period of the sequence $V_k \pmod{p}$, so the probability is well defined. If these probabilities were independent for distinct prime factors of n, then for square free n we could determine the probability that n is a pseudoprime from local contributions. These probabilities are most likely not independent.

Assume D is square free.

Before looking at these probabilities in the various cases we first recall a few facts. Fix the prime p. Let $\mathbb{F}_p$ and $\mathbb{F}_{p^2}$ denote the fields of order p and p^2, respectively. In the notation of Section 2.3,

$$\alpha = \frac{P + \sqrt{D}}{2} \qquad \beta = \frac{P - \sqrt{D}}{2}.$$

We think of these quantities as elements of $\mathbb{Q}(\sqrt{D})$, or $\mathbb{F}_{p^2}$ when $(D/p) = -1$, or $\mathbb{F}_p$ when $(D/p) = 1$.

When $(D/p) = -1$, for $x, y \in \mathbb{F}_p$ we have $(x + y\sqrt{D})^p = x - y\sqrt{D}$ in $\mathbb{F}_{p^2}$. In particular, $\alpha^p = \beta$ and $\beta^p = \alpha$. Whereas when $(D/p) = 1$, for $x, y \in \mathbb{F}_p$ we have $(x + y\sqrt{D})^p = x + y\sqrt{D}$ and $x^{p-1} = 1$ in $\mathbb{F}_p$. In particular, $\alpha^{p-1} = 1$ and $\beta^{p-1} = 1$.

These facts allow us to derive the formulas (7) and (8). Indeed if $(D/p) = -1$, then in $\mathbb{F}_{p^2}$ we have

$$U_{p+1} = \frac{\alpha^{p+1} - \beta^{p+1}}{\alpha - \beta} = \frac{\alpha\beta - \beta\alpha}{\alpha - \beta} = 0$$

and

$$V_{p+1} = \alpha^{p+1} + \beta^{p+1} = 2\alpha\beta = 2Q.$$

Since both sides are in $\mathbb{F}_p$, we may think of these congruences as congruences modulo p. These give exactly (7) and (8) with $(D/p) = -1$.

Similarly if $(D/p) = 1$, then in $\mathbb{F}_p$ we have

$$U_{p-1} = \frac{\alpha^{p-1} - \beta^{p-1}}{\alpha - \beta} = \frac{1-1}{\alpha - \beta} = 0$$

and

$$V_{p-1} = \alpha^{p-1} + \beta^{p-1} = 1 + 1 = 2.$$

We are most interested in the case $(D/n) = -1$ and composite n that satisfy $U_{n+1} \equiv 0 \pmod{n}$ and $V_{n+1} \equiv 2Q \pmod{n}$. Consequently in the following we shall focus on the case of $(D/n) = -1$. We now investigate the probabilities mentioned above.

7.1. **Case 1:** $(D/p) = -1$**.** Since $(D/p)(D/y) = (D/py) = (D/n) = -1$, we must have $(D/y) = 1$. We also have

$$U_{py+1} = \frac{\alpha^{py+1} - \beta^{py+1}}{\alpha - \beta} = \alpha\beta\frac{\beta^{y-1} - \alpha^{y-1}}{\alpha - \beta} = QU_{y-1}$$

and

$$V_{py+1} = \alpha^{py+1} + \beta^{py+1} = Q(\beta^{y-1} + \alpha^{y-1}) = QV_{y-1}.$$

Thus, for Congruences (7) and (8) we are interested respectively in the probability that $U_{y-1} \equiv 0 \pmod{p}$ and the probability that $V_{y-1} \equiv 2 \pmod{p}$.

The sequences U_y and V_y as functions of y modulo p are periodic with periods less than p^2. The condition $(D/y) = 1$ has period D (or $4D$) as we are implicitly interested in representatives for y that are odd. By the CRT this modulo D condition is irrelevant to the conditional probability unless $D \mid p^2 - 1$.

Lemma 1. *The periodicity of the appearance of 0 for the sequence U_{y-1} is exactly the order of the image of α in the group $\mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times$. In particular, it divides $p+1$.*

Moreover, the order is 2 when $P = 0 \pmod{p}$.

Proof. We recall that the sequence U_{y-1} gives the irrational part of the number α^{y-1}, and thus $U_{y-1} = 0 \pmod{p}$ if and only if $\alpha^{y-1} \in \mathbb{F}_p$. Thus the collection of y such that $U_{y-1} = 0$ is exactly the kernel of the map $\mathbb{F}_{p^2}^\times \to \mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times$. Hence, we are really studying the image of the map $\langle\alpha^n\rangle \to \mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times$. Since the image is a subgroup, its order divides $p+1$. This completes the proof of the first claim.

We note that if $P = 0 \pmod{p}$, then $\alpha = \sqrt{D}/2$ and $\alpha^2 = -Q \in \mathbb{F}_p$.

Since we know $U_{(p+2)-1} = 0$, we obtain

Proposition 1. *There exists a divisor k of $p+1$ such that $U_{py+1} \equiv 0 \pmod{p}$ if and only if $y \equiv p+2 \equiv 1 \pmod{k}$.*

In particular, the probability that $U_{py+1} \equiv 0 \pmod{p}$ is $\frac{1}{k} \geq \frac{1}{p+1}$.

If we assume additionally the y is odd then subject to this condition the probability is at least $\frac{2}{p+1}$

.

We note that in the above we are not directly accounting for the possibility that D divides k, in which case the condition $(D/y) = 1$ would tend to lead to a higher conditional probability as some of the k options for y must be discarded, but we will never discard the option 1 mod k. In particular the claim remains valid with these considerations.

Now we note that the order of α in $\mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times$ is precisely the order of $\frac{\alpha}{\beta} = \frac{\alpha^2}{Q}$ in $\mathbb{F}_{p^2}^\times$ and the condition $U_{y+1} \equiv 0 \pmod{p}$ is equivalent to $\left(\frac{\alpha^2}{Q}\right)^{y+1} = 1 \in \mathbb{F}_{p^2}^\times$. In the case n, and hence y, are odd we will always have $y+1$ even, and writing $y+1 = 2z$ the condition on z is

$$1 = \left(\frac{\alpha^2}{Q}\right)^{2z}.$$

As such we can see that this order is automatically at most $(p+1)/2$.

If we continue to write $y+1=2z$ and look at

$$1=\left(\frac{\alpha^2}{Q}\right)^{2z}=\left(\frac{\alpha^2}{-Q}\right)^{2z}.$$

we can see that the 2-part of the order of $(\alpha^2/Q)^2$ will tend to further bounded if Q or $-Q$ is a square. Though this is guaranteed when $p\equiv 3 \pmod 4$ it is also guaranteed if Q or $-Q$ is an integer perfect square.

Additionally we notice that when y is odd if we replace α,β by the conjugate pair $\alpha'=\sqrt{D}\alpha, \beta'=-\sqrt{D}\beta$ we effectively replace Q by $-DQ$ but the order of $(\alpha'/\beta')^2$ agrees with that of $(\alpha/\beta)^2$. It follows that having any of

$$Q, \quad ,-Q, \quad DQ, \quad -DQ$$

perfect integer squares will tend to increase the probability $U_{y+1}\equiv 0 \pmod p$ when y is odd. This phenomenon can be observed empirically by counting the proportion of n which are lpsp for different options P,Q. Those with Q of the above form tend to appear more than on average.

The situation for (8) is somewhat more subtle. We have the following

Lemma 2. *The period of the sequence V_{y-1} divides the order of α in $\mathbb{F}_{p^2}^{\times}$, which is a divisor of p^2-1.*

Moreover, the order of α in $\mathbb{F}_{p^2}^{\times}$ is divisible by the LCM of the order of α in the group $\mathbb{F}_{p^2}^{\times}/\mathbb{F}_p^{\times}$ and the order of Q in $\mathbb{F}_p^{\times}$, and is at most twice this amount. In particular, this period is at least as large as the period of Lemma 1.

Proof. The first claim about the period is clear given that α and β have the same period.

For the second claim we note that the order of an element is divisible by the order of its image under any homomorphism. We obtain the result by considering the map $\mathbb{F}_{p^2}^{\times}\to\mathbb{F}_{p^2}^{\times}/\mathbb{F}_p^{\times}$ as well as the norm map

$$N_{\mathbb{F}_{p^2}^{\times}/\mathbb{F}_p^{\times}}:\mathbb{F}_{p^2}^{\times}\to\mathbb{F}_p^{\times}$$

for which we have

$$N_{\mathbb{F}_{p^2}^{\times}/\mathbb{F}_p^{\times}}(\alpha)=\alpha^{p+1}=Q$$

Because the intersection of the kernels of these two maps is ± 1 we conclude that the exact order of α is either the LCM or the two quantities, or exactly twice this. (The exact order is twice this if and only if there exists z with $\alpha^z=-1 \pmod p$. This is guaranteed if Q is not a square mod p.) We note further that because we are taking the LCM of a number dividing $p+1$ and one dividing $p-1$ the LCM is almost exactly the product.

Note from the lemma above we may conclude that if $P=0$ the order of α is exactly 2 times the order of $-Q$. We also conclude that if $Q=\pm 1$, the order of α divides $2(p+1)$.

It remains the case that we cannot expect that 2 only appears once in each period. Additionally, in contrast to the previous case there is no guarantee that the appearance of 2 in the period is actually itself periodic.

Lemma 3. *Let ℓ denote the period of V_y modulo p. We have that $V_{y+m(p+1)}=Q^mV_y$ and consequently each $a\in\mathbb{F}_p^{\times}$ is repeated by V_y equally often as $Q^m a$ and hence not more than $\ell/\mathrm{ord}(\mathrm{Q})$ times within one period of $V_y \pmod p$.*

Proof.

This follows from the observation that

$$V_{y+p+1}=QV_y$$

from which we obtain a bijection between the occurrences of x and Qx. Hence, each value $0\not\equiv x \pmod p$ which occurs, does so just as often as $Qx \pmod p$ in one period.

Now we consider the map

$$\Psi : \mathbb{Z} \to \mathbb{F}_p \times \mathbb{F}_p^\times$$

given by

$$y \mapsto (V_y, N_{\mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times}(\alpha^y)) = (V_y, Q^y).$$

And note that this map has a period which is either $\mathrm{ord}(\alpha)$ or $\mathrm{ord}(\alpha)/2$

Lemma 4. *The function Ψ is exactly $2:1$ on its image, and hence each $a \in \mathbb{F}_p^\times$ is repeated by V_y no more than $2\mathrm{ord(Q)}$ times in $0 \le y \le \mathrm{ord}(\alpha)$.*

We note that the image of Ψ gives the trace and norm of α^y, hence we can recover the minimal polynomial of α^y from $\Psi(y)$. It follows that $\Psi(y_1) = \Psi(y_2)$ implies either $\alpha^{y_1} = \alpha^{y_2}$ or $\alpha^{y_1} = \beta^{y_2}$. Because ℓ divides the order of α in the first case we obtain $y_1 \equiv y_2 \pmod{\ell}$. In the second case we obtain $y_1 \equiv py_2 \equiv -y_2 \pmod{\ell}$.

Proposition 2. *The probability that $V_{py+1} \equiv 2Q \pmod{p}$ is less than the minimum of*

$$\frac{1}{\mathrm{ord(Q)}} \qquad \textit{and} \qquad \frac{2\mathrm{ord(Q)}}{\mathrm{ord}(\alpha)}.$$

We remark that

$$\frac{2\mathrm{ord(Q)}}{\mathrm{ord}(\alpha)} = \begin{cases} \frac{1}{k} & \text{if } \exists z, \alpha^z = -1 \pmod{p} \\ \frac{2}{k} & \text{otherwise} \end{cases}$$

where as before, k is the order of α in $\mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times$

We first note that this proposition gives an indication of why having $\mathrm{ord(Q)}$ large is beneficial. Moreover, it indicates why one should expect the V test to be better than the U test, and at least as good even when $Q = -1$.

We next note that in the above we are not accounting for the possibility that $D \mid \ell$, in which case the condition $(D/y) = 1$ and $(D/p) = -1$ would imply the map Ψ must be injective on relevant cases. The effect is that the conditional probabilities are still bounded by the above.

Finally we note that when we combine both the U and V conditions, and consider the conditional probability of the V condition assuming the U condition this amounts to restricting to the subsequence $y = (p+2) + kx$ for which that $U_{y-1} = 0$, then as $(\alpha - \beta)U_z + 2\beta^z = V_z$, the condition $V_{y-1} = V_{(p+2)+xk-1} = 2$ becomes

$$\beta^{(p+1)+kx} = Q(\beta^k)^x.$$

This condition is periodic in x, with period the exact order of β^k, as k is the smallest power for which $\beta^k \in \mathbb{F}_p^\times$ the order of β^k divides $p-1$ and is, up to a multiple of 2, the order of Q. In particular, if Q has a large order, the probability that the V condition is satisfied remains low independently of the U condition.

7.2. **Case 2:** $(D/p) = 1$**.** Since $(D/p)(D/y) = (D/py) = (D/n) = -1$, we must have $(D/y) = -1$. As $\alpha^p = \alpha$ and $\beta^p = \beta$ we also have

$$U_{py+1} = \frac{\alpha^{py+1} - \beta^{py+1}}{\alpha - \beta} = \frac{\alpha^{y+1} - \beta^{y+1}}{\alpha - \beta} = U_{y+1},$$

so we want to estimate the fraction of y with $(D/y) = -1$ that have $U_{y+1} \equiv 0 \pmod{p}$. Likewise we have

$$V_{py+1} = \alpha^{py+1} + \beta^{py+1} = \alpha^{y+1} + \beta^{y+1} = V_{y+1},$$

so we want to estimate the fraction of y with $(D/y) = -1$ that have $V_{y+1} \equiv 2Q \pmod{p}$.

We note that in this case $\alpha, \beta \in \mathbb{F}_p^\times$ are essentially independently chosen elements (determined by P and Q).

Lemma 5. *The sequence U_{y+1} is zero precisely when $((\alpha)\beta^{-1})^{y+1} = 1$. Hence the period of the vanishing of U_{y+1} is precisely the order of $(\alpha)\beta^{-1}$ as an element of $\mathbb{F}_p^\times$. In particular, it divides $p-1$ and the LCM of the orders of α and β. Consequently, there is a divisor k of $p-1$ such that $U_{y+1} = 0$ if and only if $y = -1 \pmod k$.*

Proof. The condition $U_{y+1} \equiv 0 \pmod p$ becomes $\alpha^{y+1} = \beta^{y+1}$ in $\mathbb{F}_p^\times$, or $(\alpha)\beta^{-1} = 1$, which proves the lemma.

If $D \mid k$, then we should consider the impact of the condition $(D/y) = -1$. In contrast to the previous case it may not be possible to have $(D/y) = -1$ and $y = -1 \pmod k$. If we assume $D \mid k$ so that $y = -1 \pmod D$, then in the case

- $D = 1 \pmod 4$ and $D > 0$ then $(D/y) = (y/D) = (-1/D) = 1$ hence the conditions are never simultaneously satisfiable.
- $D = 3 \pmod 4$ and $D > 0$ then $(D/y) = (-1/y)(y/D) = (-1/y)(-1/D) = -(-1/y)$ hence the condition is satisfiable if $y = 1 \pmod 4$. But we note that if $4 \mid k$ this is not possible.
- $D = 3 \pmod 4$ and $D < 0$ then $(D/y) = (-1/y)(y/-D) = (-1/y)(-1/-D) = (-1/y)$ hence the condition is satisfiable if $y = 3 \pmod 4$.
- $D = 1 \pmod 4$ and $D < 0$ then $(D/y) = (y/-D) = (-1/-D) = -1$ hence the condition is always satisfiable.

The above suggests $D = 1 \pmod 4$ and $D > 0$ would be ideal. We note about the above conditions, $D \mid p-1$ is only particularly likely for random n when D is small. Counts of lpsps are consistent with this expectation that small positive D have fewer lpsps.

We remark that as in the case $(D/p) = -1$ if $y + 1 = 2z$ we are considering the condition

$$1 = \left(\frac{\alpha}{\beta}\right)^{y+1} = \left(\frac{\alpha^4}{Q^2}\right)^z.$$

In the case $p \equiv 3 \pmod 4$ the 2-part of the order is already reduced to 1. However, if $p \equiv 1 \pmod 4$, we will have $-1, D, -D$ are all squares modulo p, hence if any of

$$Q, \quad -Q, \quad DQ, \quad -DQ$$

are perfect integer squares this will reduce the maximum 2-part of the order of $((\alpha)\beta^{-1})^2$ and hence increase the probability that $U_{y+1} \equiv 0 \pmod p$. In contrast if Q is not a square $((\alpha)\beta^{-1})^{(p-1)/2} \equiv (\alpha^{p-1}/Q^{(p-1)/2}) \equiv -1$. This phenomenon can be observed empirically by counting the proportion of n which are lpsp for different options P, Q. Those with Q of the above form tend to be lpsp more than on average.

Lemma 6. *The period of the V_{y+1} sequence divides the LCM of the orders of α and β. The order of Q divides the LCM of the orders of α and β, as does the order of $(\alpha)\beta^{-1}$. All of these orders divide $p-1$.*

Proof. It is clear from the definition of V_{y+1} that its period divides the periods of the two functions added to obtain it. Since $Q = \alpha\beta$, its order must divide the LCM of the orders of α and β. Likewise, the order of $(\alpha)\beta^{-1}$ divides this LCM. This completes the proof.

In contrast to the previous cases, if $Q \not\equiv 1$ or $P/2 \pmod p$, there is no guarantee that there are any solutions at all.

However, we know that

$$V_{(p-2)+\ell(p-1)+1} \equiv 2 \pmod p \quad \text{and} \quad V_{\ell(p-1)+1} \equiv P \pmod p.$$

Lemma 7. *Let t denote the order of α/β in $\mathbb{F}_p^\times$ then*

$$V_{y+mt} = (\beta^t)^m V_y$$

and hence each $a \in \mathbb{F}_p^\times$ is repeated by V_y equally often as $(\beta^t)^m a$ and hence not more than $\ell/\mathrm{ord}(\beta^t)$ times within one period of $V_y \pmod p$.

Let f denote the order of α in $\mathbb{F}_p^\times$ then

$$V_{y+mf} = V_y + \beta^y((\beta^f)^m - 1)$$

and hence each $a \in \mathbb{F}_p^\times$ is repeated by V_y equally often as $(\beta^f)^m a$ and hence not more than $\ell/\mathrm{ord}(\beta^{\mathrm{t}})$ times within one period of $V_y \pmod p$.

By symmetry each $a \in \mathbb{F}_p^\times$ is repeated by not more than $\ell/\mathrm{ord}(\alpha^{\mathrm{ord}(\beta)})$ times within one period of $V_y \pmod p$.

The proof is as in the previous case.

Now we consider the map

$$\Psi : \mathbb{Z} \to \mathbb{F}_p \times \mathbb{F}_p^\times$$

given by

$$y \mapsto (V_y, N_{\mathbb{F}_{p^2}^\times/\mathbb{F}_p^\times}(\alpha^y)) = (V_y, Q^y).$$

And note that this map has a period which divides the LCM of $\mathrm{ord}(\alpha)$ and $\mathrm{ord}(\beta)$, and equals it up to a multiple of 2.

Lemma 8. *The function Ψ is either $1:1$ or $2:1$ on its image, and hence each $a \in \mathbb{F}_p^\times$ is repeated by V_y no more than $2\mathrm{ord(Q)}$ times within for $0 \le y \le \mathrm{LCM}(\mathrm{ord}(\alpha), \mathrm{ord}(\beta))$.*

It is $1:1$ unless there exists k with $\beta = \alpha^k$ and $\alpha = \beta^k$.

The proof is as in the previous case.

Proposition 3. *The probability that $V_{py+1} \equiv 2Q \pmod p$ is less than the minimum of*

$$\frac{2\mathrm{ord(Q)}}{\mathrm{LCM}(\mathrm{ord}(\alpha), \mathrm{ord}(\beta))}, \quad \frac{\mathrm{ord}(\alpha)}{\mathrm{LCM}(\mathrm{ord}(\alpha), \mathrm{ord}(\beta))}, \frac{\mathrm{ord}(\beta)}{\mathrm{LCM}(\mathrm{ord}(\alpha), \mathrm{ord}(\beta))}, \frac{\mathrm{ord}(\alpha/\beta)}{\mathrm{LCM}(\mathrm{ord}(\alpha), \mathrm{ord}(\beta))}.$$

In contrast to the previous case it is challenging to get strong bounds on this expectation when the orders of α and β are both large. However, in that case one still expects the values of α^y and β^y to behave like uniform random variables, and hence $V_y = \alpha^y + \beta^y$ should as well.

Note also that, as in the case $(D/p) = -1$ if we were considering the conditional probability of Congruence (8) given (7), we would restrict to $y = (p-2) + x\ell$, where ℓ is the order of $(\alpha)\beta^{-1}$ so that $U_{y+1} = 0$, then as

$$(\alpha - \beta)U_z + 2\beta^z = V_z$$

the condition

$$2Q = V_{y+1} = V_{(p-2)+x\ell+1} = 2\beta^{x\ell}$$

becomes

$$Q = \beta^{x\ell}$$

which is periodic with period the order of β^ℓ, and is up to a multiple of 2 the order of $\alpha\beta = Q$. By symmetry we also obtain

$$Q = \alpha^{x\ell}$$

and taking the product of these two congruences gives

$$Q^2 = Q^{x\ell}$$

and so $x\ell = 2 \pmod{\mathrm{ord}(Q)}$. This final condition has a low probability of being satisfied if $\mathrm{ord}(Q)$ is large. And is likely impossible to satisfy if $\ell = \mathrm{ord}((\alpha)\beta^{-1})$ is not relatively prime to $\mathrm{ord}(Q)$.

Once again we can see why the V sequence probably outperforms the U sequence: the expected period of the U sequence is strictly less than $p-1$, while that of V is likely to be closer to $p-1$ as it comes from the LCM of two periods. The probability that $V_{y+1} = 2Q$ can however be less than $1/(p-1)$ since it can be 0. Realistically, one expects that the values of the V sequence occur with equal frequency, though this is not guaranteed.

In contrast to the previous case the probabilities that for fixed D and p we have $U_{y+1} = 0$ or $V_{y+1} = 2Q$ are largely not independent as they both depend on periods modulo $p-1$ and so likely

either completely conflict or completely overlap. This is consistent with the observation that there should be fewer composites satisfying (7) and (8) with $(D/n) = -1$ where most $p \mid n$ have $(D/p) = 1$.

7.3. **Both cases together.** We have seen that heuristically, if you use (8) with $(D/p) = -1$ and allow $Q = 1$ or -1 as in Method A, then the order of α divides $2(p+1)$. But if you force $|Q| > 1$ as in Method A*, then this order divides $p^2 - 1 = (p-1)(p+1)$ and probably not $2(p+1)$ or $p-1$.

Consider the BPSW probable prime test. The Fermat condition $2^{n-1} = 1 \pmod n$ basically requires that the order of 2 modulo any prime factor p of n divide $n-1$. If the order is large, as it often is, then it rarely divides $n-1$ when n has other prime factors than p. But it is not that rare; it does happen occasionally, and we get (some) pseudoprimes to base 2.

The Lucas condition (7) is trickier. With $(D/n) = 1$, it is just a Fermat test with 2 replaced by α. With $(D/n) = -1$, it operates in $\mathbb{F}_{p^2}$ and needs $n+1$ to satisfy a congruence condition modulo $p+1$ in order to report n probably prime. Such a condition modulo $p+1$ happens about as often as $p-1$ divides $n-1$, so we get occasional Lucas psps.

When we combine the Fermat and Lucas conditions, we ask for n to satisfy congruence conditions modulo both $p-1$ and $p+1$. These probabilities are not independent, but as a first approximation, each event has probability about $1/p$. The probability of both events simultaneously would be $1/p^2$. Now $\sum_p 1/p$ diverges, while $\sum_p 1/p^2$ converges. By the Borel-Cantelli lemmas, the first event (just pseudoprimes or just Lucas pseudoprimes) occurs infinitely often, while the second event (counterexample to BPSW) occurs only finitely often. (The second Borel-Cantelli Lemma requires the events be pairwise independent; the first Lemma does not have this hypothesis.)

If we consider just (8) with $(D/n) = -1$ and use a method for choosing D, P, Q that does not allow $|Q| = 1$, then we are forcing both congruence conditions on n modulo $p-1$ and $p+1$ (or at least a large divisor of $p-1$ respectively $p+1$), so the number of solutions should be finite. Of course, the fact that some orders will be proper divisors of $p-1$, $p+1$, or p^2-1 will allow some solutions, perhaps infinitely many, because the event probabilities are greater than $1/p^2$ but still less than $1/p$.

8. Are there infinitely many counterexamples to the test?

As noted earlier, no odd, composite n is known that is psp(2) and, when Method A* is used to choose P and Q, such that n is also lpsp(P, Q).

Nevertheless, if we search hard enough, we *can* find odd, composite n and Lucas parameters P and Q for which

$$\begin{aligned} 2^{n-1} &\equiv 1 \pmod n, \\ U_{n+1} &\equiv 0 \pmod n, \quad \text{and} \\ V_{n+1} &\equiv 2Q \pmod n \end{aligned}$$

are simultaneously true. One such example is $n = 341$, $P = 27$, $Q = 47$, $D = P^2 - 4Q = 541$. This example was found by testing *all possible* (P, Q) pairs $\pmod n$, something one would not do when testing n for primality.

We can also find odd, composite n along with P and Q, such that n is simultaneously *strong* psp(2), *strong* lpsp(P, Q), and vpsp(P, Q). This theorem was found empirically by testing all (P, Q) pairs $\pmod n$.

Theorem 1. *Let $n \equiv 3 \pmod 4$ be a strong pseudoprime base 2. Let $k \geq 0$ be an integer. Set $P = 2^k$ and $Q = 2^{2k-1}$. Then n is also a strong lpsp(P, Q) and a vpsp(P, Q).*

Remarks.

1. If $k = 0$, then $Q = 2^{-1} \equiv (n+1)/2 \pmod n$.

2. Examples of spsp(2) that are $\equiv 3 \pmod 4$ include *composite* Mersenne numbers of the form $2^p - 1$ where p is an odd prime [22, p. 1008].

3. Corollary 1 below shows that infinitely many n satisfy Theorem 1.

4. This proof uses the facts that n is an epsp(2) and that $n \equiv 3 \pmod 4$. However, if $n \equiv 3 \pmod 4$, then n is epsp(a) if and only if n is spsp(a) [22, Theorem 4, p. 1009].

Proof. First, $D = P^2 - 4Q = 2^{2k} - 4 \cdot 2^{2k-1} = 2^{2k} - 2 \cdot 2^{2k} = -(2^k)^2$. Because $n \equiv 3 \pmod 4$, this D has Jacobi symbol $(D/n) = (-1/n) \cdot ((2^k)^2/n) = -1$.

Write $n + 1 = d \cdot 2^s$, where d is odd. Then $s > 1$, and $2d \le (n+1)/2$. We will first prove that $V_{2d} \equiv 0 \pmod n$; by Congruence (12), this will prove that n is slpsp(P, Q).

Let α and β be the roots of the characteristic equation $x^2 - Px + Q = 0$, so that

$$\alpha = \frac{P + \sqrt{D}}{2} = \frac{2^k + \sqrt{-4^k}}{2} = 2^{k-1}(1 + i)\,,$$
$$\beta = \frac{P - \sqrt{D}}{2} = \frac{2^k - \sqrt{-4^k}}{2} = 2^{k-1}(1 - i)\,.$$

Then $V_{2d} = \alpha^{2d} + \beta^{2d}$. Because $(1 + i)^2 = 2i$, we have

$$\alpha^{2d} = \left(2^{k-1}\right)^{2d} \cdot (1 + i)^{2d} = \left(2^{2k-2}\right)^d \cdot (2i)^d = \left(2^{2k-1}\right)^d \cdot i^d\,.$$

Similarly, because $(1 - i)^2 = -2i$, we have $\beta^{2d} = \left(2^{2k-1}\right)^d \cdot (-i)^d$. Therefore,

$$V_{2d} = \alpha^{2d} + \beta^{2d} = \left(2^{2k-1}\right)^d \cdot (i^d + (-i)^d) = 0\,,$$

so n is a strong lpsp(P, Q).

We will now prove that $V_{n+1} \equiv 2Q \pmod n$. Because $n \equiv 3 \pmod 4$, we can write $n + 1 = 4M$, where M is an integer. Also, $V_{n+1} = \alpha^{n+1} + \beta^{+1}$.

Observe that $(1 + i)^4 = (1 - i)^4 = -4$. Then

$$\alpha^{n+1} = \left(2^{k-1}\right)^{n+1} \cdot (1 + i)^{4M} = \left(2^{n+1}\right)^{k-1} \cdot (1 + i)^{4M} = \left(4 \cdot 2^{n-1}\right)^{k-1} \cdot (-4)^M\,.$$

β^{n+1} has the same value. Therefore,

$$\begin{aligned} V_{n+1} = \alpha^{n+1} + \beta^{n+1} &= 2 \cdot \left(4 \cdot 2^{n-1}\right)^{k-1} \cdot (-1)^M \cdot 4^M \\ &= 2 \cdot 2^{2k-2} \cdot \left(2^{n-1}\right)^{k-1} \cdot (-1)^M \cdot 2^{2M} \\ &= 2^{2k-1} \cdot \left(2^{n-1}\right)^{k-1} \cdot (-1)^M \cdot 2^{(n+1)/2} \\ &= 2Q \cdot \left(2^{n-1}\right)^{k-1} \cdot (-1)^M \cdot 2^{(n-1)/2}\,. \end{aligned} \tag{19}$$

But $2^{n-1} \equiv 1 \pmod n$ because n is spsp(2) and is therefore a Fermat pseudoprime base 2 that satisfies Congruence (3).

Moreover, because n is spsp(2), it is therefore an Euler pseudoprime base 2, so that, by Congruence (4), $2^{(n-1)/2} \equiv \left(\frac{2}{n}\right) \pmod n$. We now separate (19) into two cases.

Case I. $n \equiv 3 \pmod 8$. Then (a), M is odd, so $(-1)^M = -1$, and (b), $(2/n) = -1$.

Case II. $n \equiv 7 \pmod 8$. Then (a), M is even, so $(-1)^M = 1$, and (b), $(2/n) = 1$.

In both cases, (19) becomes

$$V_{n+1} = 2Q \cdot \left(2^{n-1}\right)^{k-1} \cdot (-1)^M \cdot 2^{(n-1)/2} \equiv 2Q \cdot 1 \cdot (-1)^M \cdot \left(\frac{2}{n}\right) \equiv 2Q \pmod n\,.$$

Therefore, n is also vpsp(P, Q). This completes the proof of the theorem.

With this n and Q, the condition $Q^{(n+1)/2} \equiv Q \cdot (Q/n) \pmod n$ in step 5 of the enhanced primality test is also satisfied: Since n is a spsp(2), it is also an spsp(2^{2k-1}), that is, spsp(Q). Therefore n is an Euler pseudoprime to base 2: $Q^{(n-1)/2} \equiv (Q/n) \pmod n$. Multiply by Q to get the condition in step 5.

Note that the values of n in Theorem 1 are not counterexamples to our primality test, because Method A* never chooses these values of P and Q.

Before we discovered paper [26] we tried to prove on our own that there are infinitely many spsp(2) in the congruence class 3 (mod 4) and found the theorem below, which has independent interest and which needs the following lemma.

Lemma 9. *For every positive integer r there exists an integer $a \equiv 3 \pmod 4$ such that for every odd prime p, if $p \equiv a \pmod{4r}$, then r is a quadratic residue modulo p: $\left(\frac{r}{p}\right) = +1$.*

Proof. Write $r = 2^s t$ with t odd. If $t \equiv 1 \pmod 4$, let $a = 1 + 2t$. If $t \equiv 3 \pmod 4$, let $a = 4t - 1$. In either case, if s is odd, add $4t$ to a. It is easy to see that $a \equiv 3 \pmod 4$ in all cases. In the rest of the proof suppose that p is an odd prime and $p \equiv a \pmod{4r}$. Note that this implies that $p \equiv 3 \pmod 4$.

If r is a power of 4, then s is even, $t = 1$, $a = 3$ and $\left(\frac{r}{p}\right) = \left(\frac{1}{p}\right) = +1$.

If r is twice a power of 4, then s is odd, $t = 1$, $a = 7$, $8 \mid 4r$ and $\left(\frac{r}{p}\right) = \left(\frac{2}{p}\right) = +1$ by a supplement to the Law of Quadratic Reciprocity (LQR) that says that if $p \equiv 7 \pmod 8$, then $\left(\frac{2}{p}\right) = +1$.

Now suppose s is even and $t > 1$. If $t \equiv 1 \pmod 4$, then by the LQR we have

$$\left(\frac{r}{p}\right) = \left(\frac{2^s t}{p}\right) = \left(\frac{t}{p}\right) = \left(\frac{p}{t}\right) = \left(\frac{a}{t}\right) = \left(\frac{1+2r}{t}\right) = \left(\frac{1}{t}\right) = +1.$$

If $t \equiv 3 \pmod 4$, then by the LQR we have

$$\left(\frac{r}{p}\right) = \left(\frac{2^s t}{p}\right) = \left(\frac{t}{p}\right) = -\left(\frac{p}{t}\right) = -\left(\frac{4t-1}{t}\right) = -\left(\frac{-1}{t}\right) = +1.$$

Finally, suppose s is odd and $t > 1$. Then $8 \mid 4r$ and $a \equiv 7 \pmod 8$. If $t \equiv 1 \pmod 4$, then by the LQR we have

$$\left(\frac{r}{p}\right) = \left(\frac{2^s t}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{t}{p}\right) = (+1)\left(\frac{p}{t}\right) = \left(\frac{a}{t}\right) = \left(\frac{1+2t+4t}{t}\right) = \left(\frac{1}{t}\right) = +1.$$

If $t \equiv 3 \pmod 4$, then by the LQR we have

$$\left(\frac{r}{p}\right) = \left(\frac{2^s t}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{t}{p}\right) = -\left(\frac{p}{t}\right) = -\left(\frac{a}{t}\right) = -\left(\frac{4t-1+4t}{t}\right) = -\left(\frac{-1}{t}\right) = +1.$$

This completes the proof.

Theorem 2. *If $r > 1$ is an integer, there are infinitely many Carmichael numbers $m \equiv 3 \pmod 4$ that are also strong pseudoprimes to base r. Moreover, there is a constant $K > 0$ which depends on r so that the number of such $m < X$ is $\geq X^{K/(\log\log\log X)^2}$ for all sufficiently large X.*

Proof. Let $M = 4r$ and choose a by Lemma 9. Wright [29] proved that there are infinitely many Carmichael numbers $m \equiv a \pmod M$ and in fact $\geq X^{K/(\log\log\log X)^2}$ of them below X for all large enough X. Since $a \equiv 3 \pmod 4$ and $4 \mid M$, we have $m \equiv 3 \pmod 4$. In the construction of the Carmichael numbers m in the proof in [29], every prime factor p of m is odd and $\equiv a \pmod M$. Thus each $p \mid m$ satisfies $p \equiv 3 \pmod 4$ and, by Lemma 9, $\left(\frac{r}{p}\right) = +1$. By Corollary 1.2 of [3], if $\left(\frac{r}{p}\right)$ has the same value for every prime $p \mid m$, then m is a strong pseudoprime to base r. This completes the proof.

In 1980, van der Poorten and Rotkiewicz [26] proved that for every integer $r > 1$ there are infinitely many spsp(r) in every arithmetic progression $ax + b$ with $(a, b) = 1$, but they did not bound the growth rate of such numbers.

Theorem 1 of [22] asserts that for all $r > 1$ and $x > r^{15r} + 1$, there are more than $(\log x)/(4r \log r)$ strong pseudoprimes to base r less than x. Every one of these spsp(r) is $\equiv 1 \pmod 4$. Later, Pomerance [20] proved an even greater lower bound on the number of strong pseudoprimes to base r less than x. All of the spsp(r) he constructed are $\equiv 1 \pmod 4$.

Corollary 1. *Let k be a nonnegative integer. Let $P = 2^k$ and $Q = 2^{2k-1}$. Then there exist infinitely many Carmichael numbers $m \equiv 3 \pmod 4$ that are strong pseudoprimes to base 2, strong lpsp(P, Q) and vpsp(P, Q). Moreover, there is a constant $K > 0$ so that the number of such $m < X$ is $\geq X^{K/(\log\log\log X)^2}$ for all sufficiently large X.*

The corollary follows from Theorems 1 and 2.

In the case $r = 2$ all spsp(2) that we constructed in Theorem 2 are $\equiv 7 \pmod 8$. This is because when $r = 2$ Lemma 9 sets $s = t = 1$ and $a = 7$. It is easy to modify the proof of Theorem 2 to show that there are infinitely many spsp(2) that are $\equiv 3 \pmod 8$. Rather than use Lemma 9, just set $M = 8$ and $a = 3$. Then Wright's proof for this arithmetic progression constructs many Carmichael numbers $m \equiv 3 \pmod 8$, every prime factor of which is also $\equiv 3 \pmod 8$. Then the Legendre symbols $\left(\frac{2}{p}\right)$ are all -1 by a supplement to the LQR so that Corollary 1.2 of [3] still applies to show that m is spsp(2).

The smallest Carmichael number that satisfies all the conditions of this Corollary is 3 215 031 751.

Pomerance's heuristic argument.

In 1899, Korselt [16] proved that n is a Carmichael number if and only if n is square free, has at least three prime factors, and for each prime p dividing n we have $p - 1$ divides $n - 1$. As part of Erdős' heuristic argument (see [10]) that there are infinitely many Carmichael numbers (in fact more than $x^{1-\epsilon}$ up to x), he shows that there are many composite square free numbers n for which $p-1$ divides $n-1$ for each prime factor p of n. Pomerance [21] modified this argument to show that there are infinitely many strong pseudoprimes n to base 2 that are also Lucas pseudoprimes with $(D/n) = -1$. Pomerance's argument showed heuristically that there are Carmichael numbers n so that for each prime p dividing n we have $p + 1$ divides $n + 1$, and congruence conditions to ensure that n is a strong pseudoprime to base 2 and $(D/n) = (5/n) = -1$. Since the numbers n Pomerance constructed all satisfy $p - 1 \mid n - 1$ and $p + 1 \mid n + 1$ for each prime factor p of n, they satisfy all of Congruences (7)–(10).

Pomerance chooses an integer $k > 4$ and a large T. He lets $P_k(T)$ be the set of all primes p in $[T, T^k]$ such that

(1) $p \equiv 3 \pmod 8$ and the Jacobi symbol $(5/p) = -1$.
(2) $(p - 1)/2$ is square free and composed only of primes $q < T$ with $q \equiv 1 \pmod 4$.
(3) $(p + 1)/4$ is square free and composed only of primes $q < T$ with $q \equiv 3 \pmod 4$.

Let Q_1 be the product of all primes $q < T$ with $q \equiv 1 \pmod 4$. Let Q_3 be the product of all primes $q < T$ with $q \equiv 3 \pmod 4$.

Heuristically, the size of $P_k(T)$ is about $T^k/\log^2 T$.

Let ℓ be odd and let n be any product of ℓ primes $p \in P_k(T)$ such that $n \equiv 1 \pmod{Q_1}$ and $n \equiv -1 \pmod{Q_3}$.

Then $n \equiv 3 \pmod 8$, $(5/n) = -1$ and for all primes $p \mid n$ we have $p - 1 \mid n - 1$ and $p + 1 \mid n + 1$. This implies that n is a strong pseudoprime to base 2 and n satisfies all of (7)–(10), so n is a Lucas pseudoprime, a v pseudoprime, and so is a counterexample to the enhanced BPSW primality test.

The arguments of both Erdős and Pomerance were heuristic, with many unproved but plausible assumptions.

The condition $k > 4$ allows one to show that there are $x^{1-\epsilon}$ counterexamples n to the enhanced BPSW primality test with $n < x$.

The conditions $p \equiv 3 \pmod 8$ for $p \in P_k(T)$ make it easy to prove n is spsp(2).

A computer search for counterexamples to BPSW using Pomerance's construction would be very slow due partly to the conditions 2 and 3 above for primes $q < T$ and due partly to the conditions $n \equiv 1 \pmod{Q_1}$ and $n \equiv -1 \pmod{Q_3}$.

Conclusion.

In Section 7, we have presented some reasons why counterexamples to the BPSW test or to our new strengthened test should be rare or nonexistent. On the other hand, in this section we have

suggested that there might be many, perhaps infinitely many counterexamples to these tests. So which is it?

The arguments in Section 7 seem to apply to relatively small numbers, those with hundreds or thousands of decimal digits that we might actually test for primality using computers. We believe that counterexamples to either test are extremely rare among numbers of that size. The arguments in this section seem to apply to truly enormous numbers, numbers too large for even a computer to multiply. Some day, when we know more about the distribution of primes, we might be able to prove rigorously that there are infinitely many counterexamples, but these numbers might be so large that their logarithm exceeds the number of electrons in the universe.

9. Open Questions

Suppose n is composite and that we have the full factorization of n. Work by various authors has produced formulas that count or estimate:

- the number of bases a for which n is a psp(a) [5, Thm. 1], [17, Lemma 1]
- the number of bases a for which n is a spsp(a) [17, Prop. 1], [4, Thm. 1.4]
- given D, the number of P for which there is a Q such that n is lpsp(P, Q) [5, Thm. 2]
- given D, the number of (P, Q) pairs for which n is slpsp(P, Q) [4, Thm. 1.5]
- the number of (P, Q) pairs $\pmod n$ for which n is simultaneously lpsp(P, Q) and vpsp(P, Q) [12, Thm. 16].

We would like to have a formula that bounds, or better yet, counts, the number of D, or the number of (P, Q) pairs for which n is a vpsp(P, Q). We would also like to see an estimate of the asymptotic growth rate for the number of vpsp's $\leq x$; this would presumably depend on the algorithm for choosing P and Q.

References

[1] Martin R. Albrecht, Jake Massimo, Kenneth G. Paterson, and Juraj Somorovsky, *Prime and Prejudice: Primality Testing Under Adversarial Conditions*, ACM SIGSAC Conference on Computer and Communications Security, October 15-19, 2018, Toronto, Ontario, Canada, pp. 281–298, DOI 10.1145/3243734.3243787. Available at `https://eprint.iacr.org/2018/749.pdf`

[2] W. R. Alford, Andrew Granville, and Carl Pomerance, *There are Infinitely Many Carmichael Numbers*, Ann. Math. 140: pp. 703–722, doi:10.2307/2118576, JSTOR 2118576.

[3] W. R. Alford, Andrew Granville, and Carl Pomerance, *On the Difficulty of Finding Reliable Witnesses*, in *Algorithmic Number Theory (Ithaca, NY, 1994)*, Lecture Notes in Computer Science, 877 (Springer, Berlin, 1994), pp. 1–16.

[4] F.Arnault. *The Rabin-Monier theorem for Lucas pseudoprimes*, Math. Comp., vol. 66 (1997) no. 218, 869–881.

[5] Robert Baillie and Samuel S. Wagstaff, Jr., *Lucas Pseudoprimes*, Math. Comp., vol. 35 (October, 1980), no. 152, 1391–1417.
`https://doi.org/10.2307/2006406`
`http://mpqs.free.fr/LucasPseudoprimes.pdf`

[6] Robert Baillie, Andrew Fiori, and Samuel S. Wagstaff, Jr., *Strengthening the Baillie-PSW primality test*, `https://arxiv.org/abs/2006.14425`

[7] David Bressoud and Stan Wagon, *A Course in Computational Number Theory*, Wiley, 2008.

[8] John Brillhart, D. H. Lehmer, and J. L. Selfridge, *New Primality Criteria and Factorizations of* $2^m \pm 1$, Math. Comp., vol. 29 (April, 1975), no. 130, pp. 620–647. DOI 10.2307/2005583

[9] Richard Crandall and Carl Pomerance, *Prime Numbers: A Computational Perspective* 2nd edition, Springer: New York, 2005.

[10] P. Erdős. *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen, vol. 4 (1956), 201–206.

[11] Jan 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`

[12] Andrew Fiori and Andrew Shallue, *Average liar count for degree-2 Frobenius pseudoprimes*, Math. Comp., vol. 89 (2020), 493–514, DOI 10.1090/mcom/3452,
https://arxiv.org/abs/1707.05002, ver. 2, April, 2020.
[13] Jon Grantham, *A Probable Prime Test With High Confidence*, J. Number Theory, vol. 72 (September, 1998), no. 1, 32–47.
http://www.sciencedirect.com/science/article/pii/S0022314X98922478
[14] Jon Grantham, *Frobenius Pseudoprimes*, Math. Comp., vol. 70 (2001), no. 234, 873–891. https://doi.org/10.1090/S0025-5718-00-01197-2
[15] Dana Jacobsen, *Pseudoprime Statistics, Tables, and Data*.
http://ntheory.org/pseudoprimes.html
The counts of lpsp and slpsp to 10^{15} from method A (or A*) are given in the columns labeled "#LPSP Lucas-Selfridge OEIS A217120" and "#SLPSP Strong Lucas-Selfridge OEIS A217255".
[16] A. Korselt, Probléme chinois. *L'Intermédiaire des Mathématiciens*, 6:142–143, 1899.
[17] L. Monier, *Evaluation and comparison of two efficient primality testing algorithms*, Theoretical Computer Science, vol. 12 (1980), pp. 97–108.
[18] Richard Pinch, *The Carmichael numbers up to* 10^{21}, Anne-Maria Ernvall-Hytönen, Matti Jutila, Juhani Karhumäki, Arto Lepistö (Eds.), Proceedings of Conference on Algorithmic Number Theory, TUCS General Publication, Turku Centre for Computer Science, pp. 129-131, 2007.
https://tucs.fi/publications/attachment.php?fname=G46.pdf
[19] Richard Pinch, *The Carmichael numbers up to* 10^{18}. https://arxiv.org/abs/math/0604376
[20] Carl Pomerance, *A New Lower Bound for the Pseudoprime Counting Function*, *Illinois J. Math.*, vol. 26, no. 1, 1982, pp. 4–9.
https://math.dartmouth.edu/~carlp/PDF/lower.pdf
[21] Carl 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.
https://www.math.dartmouth.edu/~carlp/dopo.pdf
[22] Carl Pomerance, J. L. Selfridge, and Samuel S. Wagstaff, Jr., *The Pseudoprimes to* $25 \cdot 10^9$, *Math. Comp.*, vol. 35, no. 151, July, 1980, pp. 1003–1026.
https://doi.org/10.1090/S0025-5718-1980-0572872-7 ,
https://math.dartmouth.edu/~carlp/PDF/paper25.pdf
[23] Michael O. Rabin, *Probabilistic Algorithm for Testing Primality*, Journal of Number Theory, vol. 12, no. 1, 1980, pp. 128–138. https://doi.org/10.1016/0022-314X(80)90084-0
[24] Andrzej Rotkiewicz, *Lucas and Frobenius Pseudoprimes*, Annales Mathematicae Silesianae, vol. 17, 2003, pp. 17–39,
available at http://www.sbc.org.pl/Content/33711/2003_03.pdf
[25] Douglas B. Staple, *The Combinatorial Algorithm for Computing* $\pi(x)$, Master's Degree Thesis at Dalhousie University, August, 2015.
https://arxiv.org/abs/1503.01839
[26] A. J. van der Poorten and A. Rotkiewicz, *On Strong Pseudoprimes in Arithmetic Progressions*, *J. Austral. Math. Soc. (Series A)* 29 (1980), pp. 316–321.
[27] H. C. Williams. On numbers analogous to the Carmichael numbers. *Canad. Math. Bull.*, 20:133–143, 1977.
[28] H. C. Williams. *Édouard Lucas and primality testing*. Wiley, New York, New York, 1998.
[29] Thomas Wright, *Infinitely many Carmichael Numbers in arithmetic progressions*, *Bull. London Math. Soc.* 45 (2013), pp. 943–952.

Appendix A. Appendix. Methods A and A* generate the same lpsp lists

Recall that a Lucas probable prime is a solution n to (1). Here we prove that Methods A and A* give the same solutions. We also prove a similar result for strong Lucas probable primes. In this appendix we write $U_n(P, Q)$ and $V_n(P, Q)$ for the two Lucas sequences with parameters P, Q.

Theorem 3. *Let n be a positive integer relatively prime to 10. Then n is a Lucas probable prime for Method A if and only if it is a Lucas probable prime for Method A*.*

Proof. Methods A and A* differ only when $D = 5$. With that D, Method A sets $P = 1$, $Q = -1$, while A* sets $P = Q = 5$. Let

$$\alpha_1 = \frac{1+\sqrt{5}}{2} \quad \text{and} \quad \beta_1 = \frac{1-\sqrt{5}}{2}$$

be the two roots of $x^2 - x - 1 = 0$ and let

$$\alpha_2 = \frac{5+\sqrt{5}}{2} \quad \text{and} \quad \beta_2 = \frac{5-\sqrt{5}}{2}$$

be the two roots of $x^2 - 5x + 5 = 0$. Then

$$\alpha_2^2 = 5\left(\frac{3+\sqrt{5}}{2}\right) = 5\alpha_1^2 \quad \text{and} \quad \beta_2^2 = 5\left(\frac{3-\sqrt{5}}{2}\right) = 5\beta_1^2. \tag{20}$$

Since $\alpha_1 - \beta_1 = \sqrt{5} = \alpha_2 - \beta_2$, we have

$$U_{2k}(5,5) = \frac{\alpha_2^{2k} - \beta_2^{2k}}{\alpha_2 - \beta_2} = 5^k\left(\frac{\alpha_1^{2k} - \beta_1^{2k}}{\alpha_1 - \beta_1}\right) = 5^k U_{2k}(1,-1).$$

Now n is odd, so we can write $n+1 = 2k$; by the previous expression,

$$U_{n+1}(5,5) = 5^{(n+1)/2} U_{n+1}(1,-1).$$

Since n is not a multiple of 5, $U_{n+1}(5,5) \equiv 0 \pmod{n}$ if and only if $U_{n+1}(1,-1) \equiv 0 \pmod{n}$. This completes the proof.

Now we prove the analogue of this theorem for the strong lprp test.

Theorem 4. *Let n be a positive integer relatively prime to 10. Then n is a strong Lucas probable prime for Method A if and only if it is a strong Lucas probable prime for Method A*.*

Proof. Let α_1, α_2, β_1, β_2 be as in the proof of the previous theorem. We will prove that

$$U_{2k+1}(5,5) = 5^k V_{2k+1}(1,-1), \tag{21}$$

$$V_{2k+1}(5,5) = 5^{k+1} U_{2k+1}(1,-1), \quad \text{and} \tag{22}$$

$$V_{2k}(5,5) = 5^k V_{2k}(1,-1), \tag{23}$$

Using Equation (20), the left side of (21) is

$$\frac{\alpha_2^{2k+1} - \beta_2^{2k+1}}{\alpha_2 - \beta_2} = \frac{5^k}{\alpha_2 - \beta_2}\left(\alpha_1^{2k}\alpha_2 - \beta_1^{2k}\beta_2\right) = \frac{5^k}{\sqrt{5}}\left(\alpha_1^{2k+1}\frac{\alpha_2}{\alpha 1} - \beta_1^{2k+1}\frac{\beta_2}{\beta_1}\right).$$

Now

$$\frac{\alpha_2}{\alpha_1} = \frac{5+\sqrt{5}}{1+\sqrt{5}} = \sqrt{5} \quad \text{and} \quad \frac{\beta_2}{\beta_1} = \frac{5-\sqrt{5}}{1-\sqrt{5}} = -\sqrt{5},$$

so the left side of (21) becomes

$$\frac{5^k}{\sqrt{5}}\left(\alpha_1^{2k+1}\sqrt{5} - \beta_1^{2k+1}(-\sqrt{5})\right) = 5^k\left(\alpha_1^{2k+1} + \beta_1^{2k+1}\right),$$

which is the right side of (21). Equation (22) is proved the same way. Equation (23) is even easier:

$$V_{2k}(5,5) = \alpha_2^{2k} + \beta_2^{2k} = (5\alpha_1)^{2k} + (5\beta_1)^{2k} = 5^k(\alpha_1^{2k} + \beta_1)^{2k} = 5^k V_{2k}(1,-1).$$

Now if n is an slprp(1,−1) because $V_d(1,-1) \equiv 0 \pmod{n}$, then Equation (21) shows that n is an slprp(5,5) because $U_d(5,5) \equiv 0 \pmod{n}$, and vice versa. Also if n is an slprp(1,−1) because $U_d(1,-1) \equiv 0 \pmod{n}$, then Equation (22) shows that n is an slprp(5,5) because $V_d(5,5) \equiv 0 \pmod{n}$, and vice versa. Finally, if n is an slprp(1,−1) because $V_{d2^s}(1,-1) \equiv 0 \pmod{n}$ for some

$0 < s < d$, then Equation (23) shows that n is an slprp(5,5) because $V_{d2^s}(5,5) \equiv 0 \pmod{n}$, and vice versa. This completes the proof.

State College, PA USA
Email address, Robert Baillie: rjbaillie@frii.com

Mathematics and Computer Science, 4401 University Drive, University of Lethbridge, Lethbridge, Alberta, T1K 3M4 Canada
Email address, Andrew Fiori: andrew.fiori@uleth.ca

Center for Education and Research in Information Assurance and Security and Department of Computer Sciences, Purdue University, West Lafayette, IN 47907-1398 USA
Email address, Samuel S. Wagstaff, Jr.: ssw@cerias.purdue.edu