LOOKING FOR FIBONACCI BASE-2 PSEUDOPRIMES

DANIEL J. MONFRE AND DOMINIC KLYVE

Abstract. In this paper, we examine computationally the results of combining two well-known, simple, and imperfect tests for primality: the Fermat base-2 test, and the Fibonacci test. Although considerable attention has been paid to various properties of composite integers which pass the base-2 test (*base-2 pseudoprimes*), no comparable study of Fibonacci and base-2 Fibonacci tests exists in the literature. Our study tabulates various empirical properties of these numbers. Among other things, we conclude that there are no base-2 Fibonacci pseudoprimes less than 10^{15} which are congruent to 2 or 3 (modulo 5).

1. Introduction

Several primality tests are based on the simple expedient of taking the converse of theorems about primes. Perhaps the most famous of these arises from Fermat's little theorem, which states (as a special case) that

$$2^{p-1} \equiv 1 \pmod{p} \tag{1}$$

for any odd prime p. Its converse gives us the following test.

Primality Test 1.1 (Base-2 Fermat test). *For a given integer $n > 1$, compute $2^{n-1} \pmod{n}$. If the result is 1, return "probable prime." Otherwise, return "composite."*

The test is not perfect; in addition to returning *probable prime* for all prime integers, it sometimes returns *probable prime* for composite integers. A composite number n that "passes" the test (that is, for which the test returns "probable prime") is said to be a *base-2 pseudoprime*. It is known that there are infinitely many base-2 pseudoprimes [1], the smallest of which is $341 = 11 \cdot 31$.

A second theorem about primes concerns, a bit surprisingly, the Fibonacci numbers. If we let F_i denote the ith number in the Fibonacci sequence $1, 1, 2, 3, 5, \ldots$ (where $F_0 = 0$), then the following theorem holds (see [4] for a proof).

Theorem 1.2 (Fibonacci primality theorem)**.** *If n is prime, then*

$$F_{n-(n|5)} \equiv 0 \pmod{n}, \tag{2}$$

where $(n|5) = \left(\frac{n}{5}\right)$ denotes the Legendre symbol; that is,

$$\left(\frac{n}{5}\right) = \begin{cases} 1 & \text{if } n \equiv \pm 1 \pmod{5} \\ -1 & \text{if } n \equiv \pm 2 \pmod{5} \\ 0 & \text{if } n \equiv 0 \pmod{5}. \end{cases}$$

As with the base-2 test, we can take the converse of this theorem and use it as a primality test, (although it ends up being more useful to restrict to the case of integers coprime to 5).

Primality Test 1.3 (Fibonacci primality test)**.** *Given a positive integer n with $(n, 5) = 1$, compute $F_{n-(n|5)} \pmod{n}$. If the result is 0, return "probable prime." Otherwise, return "composite."*

Just as the base-2 test was a special case of a more general test which allows 2 to be replaced with any number base, the Fibonacci primality test is a special case of a more general test which allows the Fibonacci sequence to be replaced by an arbitrary Lucas sequence (see [6] for more information, and [4] for additional discussion and a proof of the general theorem). Also, as was the case with the base-2 test, the Fibonacci test is far from perfect; once again, there are infinitely many Fibonacci pseudoprimes [7], the first of which is $323 = 17 \cdot 19$.

Both of these tests run quite quickly (in fact, each can test an integer n in $O(\log n)$ arithmetic operations), but the failure rate for each is too high to use in practice (see Table 3). However, we might expect considerably more success if we were to combine the tests into one large, stronger test.

Primality Test 1.4. *[The Fibonacci Base-2 Primality Test] Given an integer n,*

(1) *Subject n to a base-2 primality test. If that test returns composite, return "composite" and stop. Else go to step 2.*
(2) *Subject n to a Fibonacci primality test. If this test returns composite, return "composite." Else, return "probable prime."*

This test combines the identification power of both Tests 1.1 and 1.3, and we expect that it will be considerably stronger than either test alone. In fact, we might hope (if a bit naively) that no composite integers will pass Primality Test 1.4. Alas, this is not the case: there are still infinitely many Fibonacci Base-2 pseudoprimes, the smallest of which is $6601 = 7 \cdot 23 \cdot 41$. It turns out, however, that a study of the properties of these base-2 Fibonacci pseudoprimes reveals some curious information about their distribution.

2. Earlier Computational Work

2.1. **Base-2 pseudoprimes (psp(2)'s).** The computation of base-2 pseudoprimes (psp(2)'s) has a long history, dating back to at least 1820 when Sarrus noted that the composite number 341 was a solution to Fermat's little theorem. The advent of computers has led to comprehensive searches for psp(2)'s, the current record being an enumeration of all psp(2)'s not greater than 10^{15} [5] (see also [8] for important searches with important milestones and statistics). Beginning with [8], these searches involved the clever use of theorems about psp(2)'s to limit the search space – that is, not every composite number needed to be tested.

2.2. **Fibonacci pseudoprimes (fpsp's).** By constrast, the Fibonacci pseudoprimes (fpsp's) are comparative newcomers on the scene. They were first defined by Emma Lehmer in 1964 [7], who proved in the same paper that there exist infinitely many fpsp's. Much less has been proven about fpsp's, and computational searches for these numbers are correspondingly less comprehensive. The most intensive previous search known to us was conducted by Peter Anderson [2], who found all fpsp's less than 2,217,967,487.

2.3. **Base-2 Fibonacci pseudoprimes (fpsp(2)'s).** Beginning with the work of Pomerance, Selfridge, and Wagstaff [8], some computational work has been expended on finding those composite integers which are both psp(2)'s and fpsp's. These *base-2 Fibonacci pseudoprimes* (fpsp(2)'s) are comparatively rare, but still exist in large enough numbers to obviate the immediate utility of any primality test based on these tests. However, Pomerance et al. noted that none of the fpsp(2)'s yet found is congruent to 2 or 3 modulo 5. The authors of [8] offered a \$30 prize for the first such integer found. This prize, which has since been increased to \$620 with the three offering (\$20 + \$100 + \$500) for the first integer found, or (\$500 + \$100 + \$20) for a proof that no such integer exists.

2.4. **Present work and computational methods.** Our work involves extending Anderson's fpsp search by a factor of more than 200 and compiling statistical information about fpsp's and fpsp(2)'s. Because our primary concern was an extension of the search bound for fpsp's, we first searched the range $[1, 5 \cdot 10^{11}]$ for fpsp's, and then from that set of fpsp's, we applied the base-2 test to find all the fpsp(2)'s. A second data set of fpsp(2)'s was generated using Galway's data on psp(2)'s up to 10^{15}. We acquired Galway's data, and checked each pseudoprime for fpsp status. We thereby acquired two datasets: a smaller set of all integers up to $5 \cdot 10^{11}$ which are fpsp's, psp(2)'s, or fpsp(2)'s, and a largest set of all integers up to 10^{15} which are psp(2)'s and fpsp(2)'s.

All of our computations were performed using PARI/gp. Checking equation (1) was done by using the built-in binary ladder for modular exponentiation. To check whether our integers satisfied equation (2), and were therefore candidates for being fpsp's, we needed a method to calculate $F_{n-(n|5)} \pmod{n}$. Following a suggestion of Peter Anderson, we used a simple method based on an elementary identity concerning matrix exponentiation and Fibonacci numbers, namely:

Theorem 2.1. *Let F_n be, as before, the nth Fibonacci number. Then*

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n = \begin{pmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{pmatrix}.$$

By considering the matrix entries $\pmod{n}$, the matrix exponentiation was carried out in time $O(\log n)$ using the same binary ladder technique used in the base-2 test. We were able thereby to test even "large" integers for their fpsp status quite easily. Our code ran on a computer in a lab at Carthage College, over weekends and during other periods of low use. The machines were Windows PC's with 2.8GHz Pentium processors, and tested all integers coprime to 5 for fpsp status. In practice, we found we could search a range of a billion integers in about 24 hours, so that our entire computation (minus separate runs to double-check certain ranges of our calculation) consumed about 500 CPU days.

3. Results

We begin with a simple enumeration of pseudoprimes up to a given bound, (Table 3), giving an idea of the efficacy of combining the two tests.

x	fpsp's	psp(2)'s	fpsp(2)'s
10^3	2	3	0
10^4	9	22	1
10^5	50	78	4
10^6	155	245	15
10^7	511	750	50
10^8	1460	2057	134
10^9	4152	5597	377
10^{10}	11049	14884	968
10^{11}	29334	38975	2517
5×10^{11}	**57238**	**76242**	**4734**
10^{12}		101629	6222
10^{13}		264239	15589
10^{14}		687007	38749
10^{15}		1801533	98116

(3)

Table 3. Number of pseudoprimes less than x.

Here we quickly see that the base-2 Fibonacci tests, when combined, are quite powerful. Fewer than $100,000$ integers are pseudoprimes up to 10^{15}; that is, the probability of a composite integer less than 10^{15} being a fpsp(2) is about 1 in 3×10^8.

Recalling the observation of Pomerance et al., however, we note that of even more interest than the count may be the distribution of pseudoprimes in residue classes.

k	all composites	fpsp's		psp(2)'s		fpsp(2)'s	
	%	#	%	#	%	#	%
2	13	33792	59	34373	23	2309	50
3	21	6478	11	8007	54	665	14
4	23	8144	14	13562	9	894	19
5	19	6733	12	14168	10	678	14
6	12	1922	3	5465	4	152	3
7	7	167	0.3	648	0.4	17	0.3
8	3	2	0	17	0	0	0
9	1	0	0	0	0	0	0

Number and percentage of numbers below $5 \cdot 10^{11}$
with exactly k prime divisors.

4. The distribution of pseudoprimes in residue classes

Table 4 gives the distribution of psp(2)'s, fpsp's, and fpsp(2)'s up to 5×10^{11} in various residue classes, together with the same information for psp(2)'s and fpsp(2)'s up to 10^{15}. Looking at this data, it is easy to observe that for any n, the largest residue class seems to be $1 \pmod{n}$. Following the example of [8], we have computed a similar table for all moduli ≤ 200.

For 178 of these 200 moduli, the residue class $1 \pmod{m}$ contains the largest number of fpsp's. The smallest modulus which serves as a counterexample is $m = 41$, in which there are 2563 fpsp(2)'s in $0 \pmod{41}$, and only 2115 in $1 \pmod{41}$. In the set of fibpsp(2)'s up to 10^{15}, the smallest residue class for which $1 \pmod{m}$ is not the largest class mod m is $m = 31$, for which there are 6790 fpsp(2)'s which are $0 \pmod{31}$, and 6778 which are $1 \pmod{31}$.

The following table lists the number of pseudoprimes by residue class.

		Less than 5×10^{11}			Less than 10^{15}	
Modulus	Class	fpsp's	psp(2)'s	fpsp(2)'s	psp(2)'s	fpsp(2)'s
3	0	792	1789	14	20607	66
3	1	35794	64908	4298	1547871	87896
3	2	20652	9545	422	233055	10154
4	1	34803	67670	4305	1603709	87818
4	3	22435	8572	429	197824	10298
5	0	0	4417	0	69477	0
5	1	34882	45519	4586	1123305	94620
5	2	9103	9470	0	224513	0
5	3	8283	9225	0	212523	0
5	4	4970	7611	148	171715	3496
6	1	35794	64908	4298	1547871	87896
6	3	792	1789	14	20607	66
6	5	20652	9545	422	233055	10154
7	0	2317	6553	130	119752	1694
7	1	19189	31621	2200	807226	46386
7	2	6128	7162	349	160842	6270
7	3	6509	8364	718	193593	16460
7	4	5856	6936	339	156600	6354
7	5	6356	7774	428	180257	8391
7	6	10883	7832	570	183263	12561
8	1	23594	45147	2703	1090108	55082
8	3	8912	4258	213	98976	5116
8	5	11209	22523	1602	513601	32736
8	7	13523	4314	216	98848	5182
9	1	21541	40895	2927	1004546	60831
9	2	5168	3242	152	77457	3361
9	3	415	895	4	10260	35
9	4	7162	11923	699	271353	13616
9	5	5109	3138	133	77914	3398
9	6	377	894	10	10347	31
9	7	7091	12090	672	271972	13449
9	8	10375	3165	137	77684	3395
12	1	26421	57758	3890	1385497	78321
12	3	111	69	0	585	0
12	5	7701	8192	401	198190	9431
12	7	9373	7150	408	162374	9575
12	9	681	1720	14	20022	66
12	11	12951	1353	21	34865	723

5. Relationship to other primality tests

For many practical purposes, it is convenient to have a very fast primality test, even if it may occasionally gives wrong information (e.g., it declares that a composite number is prime). Perhaps the most frequently used primality test today is the BPSW test, which involves modifications by Baille and Wagstaff [3] to the work of Pomerance, Selfridge, and Wagstaff described above [8]. The test has been described in several similar related forms, but the canonical statement is probably the following test.

Primality Test 5.1 (BPSW Primality Test)**.** *Given an integer n,*

(1) *Perform a* strong *base-2 pseudoprime test on n (see below).*
(2) *If n passes the test above, find the first a in the sequence* 5*,* -7*,* 9*,* -11*, ... for which the Jacobi symbol* $\left(\frac{a}{n}\right) = -1$*. Then, perform a Lucas pseudoprimality test with discriminant a on n.*
(3) *If n passes this test also, return "probable prime."*

For the purposes of the current article, it suffices to think of step one as a slightly slower (but more rigorous) version of our Base-2 test, and step 2 as a similar analog to our Fibonacci test. Much has been written about this test, which to date has no known exceptions. For more detailed information about the BPSW test, see [3, 4]. Like the Base-2 and Fibonacci tests, the BPSW test runs on time $O(\log n)$. However, in practice it requires more bit operations than the base-2 Fibonacci described in this work. There may, therefore, be some time savings to be found in deterministic programs which determine the primality of many small integers (that is, those not greater than 10^{15}), by replacing the standard BPSW test with one that uses the base-2 Fibonacci test for integers congruent to 2 or 3 modulo 5.

6. Distribution of pseudoprimes according to number of prime divisors

Table 1 gives the number of Fibonacci pseudoprimes, base-2 pseudoprimes, and Fibonacci/base-2 pseudoprimes below $5 \cdot 10^{11}$ which have exactly k distinct prime factors.

The percentage of all composites with k prime factors was calculated via the formula $\Pi_k(x)/(x - \Pi_1(x))$, with $x = 5 \times 10^{11}$, where $\Pi_k(x)$ is the count of integers not greater than x with exactly k prime factors (counting multiplicity). We used the asymptotic estimate

$$\Pi_k(x) \sim \frac{x}{\log x} \frac{(\log \log x)^{k-1}}{(k-1)!}.$$

We find the same strange results that were reported in [8] – namely, that there are a lot of pseudoprimes with two prime factors, and more with four or five prime factors than there are with three. Like the authors of the previous work, we have no idea why this should be.

7. Acknowledgements

We wish to thank Matt Brzeski and the staff of the My Carthage Resource Center for expert assistance in setting up the computer network for our computation. Dominic Klyve was partially supported by a Carthage College Summer Undergraduate Research Experience grant, and Dan Monfre was fully supported by the same grant.

References

[1] W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers*, Ann. of Math. (2), **139.3** (1994), 703–722.

[2] P. G. Anderson, *Fibonacci pseudoprimes under 2,217,967,487 and their factors*, `http://www.cs.rit.edu/usr/local/pub/pga/fibonacci_pp`.

[3] R. Baillie and S. S. Wagstaff, Jr., *Lucas pseudoprimes*, Math. Comp. **35.153** (1980), 1391–1417.

[4] R. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, 2nd ed., Springer, New York, 2005.

[5] W. Galway, *Tables of pseudoprimes and related data*, `http://www.cecm.sfu.ca/Pseudoprimes/`.

[6] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Problem Books in Mathematics, Springer-Verlag, New York, 2004.

[7] E. Lehmer, *On the infinitude of Fibonacci pseudoprimes*, The Fibonacci Quarterly, **2.3** (1964), 229–230.

[8] C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr., *The pseudoprimes to* $25 \cdot 10^9$, Math. Comp., **35.151** (1980), 1003–1026.

MSC2010: 11A41, 11Y11

Department of Mathematics, Carthage College, 2001 Alford Drive, Kenosha, WI 53140

E-mail address: `daniel.monfre@gmail.com`

Department of Mathematics, Central Washington University, 400 East University Drive, Ellensburg, WA 98926

E-mail address: `klyved@cwu.edu`