USING FIBONACCI FACTORS TO CREATE FIBONACCI PSEUDOPRIMES

JOHN GREENE, JUNHYUN LIM, SHAUNAK MASHALKAR, AND EDWARD F. SCHAEFER

ABSTRACT. Carmichael showed for sufficiently large L, F_L has at least one prime divisor p such that $p \equiv \pm 1 (\mathrm{mod}\, L)$. For a given F_L, we will show that a product of distinct odd prime divisors with this congruence condition is a Fibonacci pseudoprime. As a byproduct, this result leads to a proof of the presumably known result that if L is prime and F_L is composite, then F_L is a Fibonacci pseudoprime. Such pseudoprimes can be used in an attempt, here unsuccessful, to find an example of a Baillie-PSW pseudoprime, i.e., an odd Fibonacci pseudoprime n such that $n \equiv \pm 2 (\mathrm{mod}\, 5)$ and is also a base-2 pseudoprime.

1. INTRODUCTION

For all odd prime numbers p we have $p | F_{p-(\frac{5}{p})}$, where $(\frac{5}{p})$ is the Legendre symbol. This is well-known and can be proved using the lemmas in Section 2. An odd composite integer n is said to be a Fibonacci pseudoprime if $n | F_{n-(\frac{5}{n})}$, where $(\frac{5}{n})$ is the Jacobi symbol, which generalizes the Legendre symbol. Here are the six smallest Fibonacci pseudoprimes, their prime factorizations, and the smallest positive Fibonacci number that each divides: $323 = 17 \cdot 19 | F_{18}$, $377 = 13 \cdot 29 | F_{14}$, $1891 = 31 \cdot 61 | F_{30}$, $3827 = 43 \cdot 89 | F_{44}$, $4181 = 37 \cdot 113 | F_{19}$, and $5777 = 53 \cdot 109 | F_{27}$. For each of the six smallest Fibonacci pseudoprimes n, if F_L is the smallest positive Fibonacci number for which n is a divisor (i.e., $L = \mathrm{ord}_f(n)$), then each prime divisor p_i of n satisfies $p_i \equiv \pm 1 (\mathrm{mod}\, L)$. This is not always the case. The seventh smallest Fibonacci pseudoprime is $6601 = 7 \cdot 23 \cdot 41 | F_{120}$ and none of its prime divisors p_i satisfy $p_i \equiv \pm 1 (\mathrm{mod}\, 120)$. Nevertheless, we can use the above observation to create many Fibonacci pseudoprimes. We construct them using the theorem below.

Theorem 1.1. *Let L be a positive integer. For some $k \geq 2$, let $p_1, \ldots, p_k$ be distinct odd primes dividing F_L with the property that for each i we have $p_i \equiv \pm 1 (\mathrm{mod}\, L)$, assuming at least two such primes exist. Then, $P := \prod_{i=1}^{k} p_i$ is a Fibonacci pseudoprime.*

It seems common for prime divisors p_i of F_L to satisfy $p_i \equiv \pm 1 (\mathrm{mod}\, L)$. For example, four of the prime divisors of F_{100} are 101, 401, 3001, and 570601 and F_{7560} has 30 prime divisors p_i that satisfy $p_i \equiv \pm 1 (\mathrm{mod}\, 7560)$. It follows from Proposition 2.10 that because $5 | 7560$, all prime divisors p_i of F_{7560} that satisfy $p_i \equiv \pm 1 (\mathrm{mod}\, 7560)$ satisfy $p_i \equiv 1 (\mathrm{mod}\, 7560)$. All Fibonacci numbers up to F_{1408} have been factored completely and complete or partial factorizations of F_L for $1409 \leq L \leq 9999$ have been given (see [1]). For $1 \leq L \leq 1408$, the average number of odd prime divisors p_i of F_L that satisfy $p_i \equiv \pm 1 (\mathrm{mod}\, L)$ is $7279/1408 \approx 5.17$.

Applying Theorem 1.1 to the fully and partially factored Fibonacci numbers F_L for $1 \leq L \leq 9999$, we can create approximately 2^{31} Fibonacci pseudoprimes. However, they will not all be distinct. For example, $F_{19} = 4181 = 37 \cdot 113$. Not only do both prime divisors p_i satisfy $p_i \equiv \pm 1 (\mathrm{mod}\, 19)$, they both satisfy $p_i \equiv \pm 1 (\mathrm{mod}\, 38)$. So the Fibonacci pseudoprime 4181 will appear for both $L = 19$ and $L = 38$. If L is odd and a Fibonacci pseudoprime can be created from odd prime divisors p_i of F_L that satisfy $p_i \equiv \pm 1 (\mathrm{mod}\, L)$, the same Fibonacci pseudoprime

will arise from prime divisors of F_{2L}, as odd prime divisors p_i that satisfy $p_i \equiv \pm 1 (\mathrm{mod}\, L)$ also satisfy $p_i \equiv \pm 1 (\mathrm{mod}\, 2L)$. After removing repetitions, we are still left with approximately 2^{31} distinct Fibonacci pseudoprimes.

One reason for the appearance of such prime divisors of Fibonacci numbers comes from [3], Theorem XXVI. Carmichael proved that for every $L \neq 1, 2, 5, 6, 12$, there is a prime divisor $p \equiv \pm 1 (\mathrm{mod}\, L)$ of F_L, which divides no F_K for $K < L$. We leave it to the analytic number theorists to study the expected number of prime divisors p_i of F_L that satisfy $p_i \equiv \pm 1 (\mathrm{mod}\, L)$ as a function of L.

In Section 2, we prove Theorem 1.1. This theorem provides a new way of creating Fibonacci pseudoprimes and thus can be added to the list of methods for constructing them found in [4], [6], [10], [13], [18], and [19]. We can use this theorem to prove Proposition 2.9, which states that if L is prime and F_L is composite, then F_L is a Fibonacci pseudoprime. The authors are not aware of a reference for this result. Its similarity to Emma Lehmer's result (see [10]) that for $L > 5$ and prime, F_{2L} is a Fibonacci pseudoprime leads us to believe that the result is known.

There is much interest in finding an integer that is an odd Fibonacci pseudoprime n such that $n \equiv \pm 2 (\mathrm{mod}\, 5)$, and is simultaneously a base-2 pseudoprime. These are sometimes referred to as Baillie-PSW pseudoprimes. There is a heuristic argument that an example exists (see [4], which refers to ideas in [14]). However, no example is known and there is a \$620 prize (payable by Carl Pomerance, Sam Wagstaff, and the Number Theory Foundation, see [15]) for those who find an example, or prove that none exists. In Section 3, we discuss how we used Theorem 1.1 and Proposition 2.9 in an unsuccessful attempt at finding an example.

2. Proof of the Theorem

We will use the following five well-known lemmas. Lemmas 2.1 and 2.2 are proven in [11], pp. 296-297.

Lemma 2.1. *Let $p \equiv \pm 1 (\mathrm{mod}\, 5)$ be prime. Then, $p | F_{p-1}$.*

Lemma 2.2. *Let $p \equiv \pm 2 (\mathrm{mod}\, 5)$ be prime. Then, $p | F_{p+1}$.*

Lemma 2.3 is proven in [9], p. 35.

Lemma 2.3. *Let m, n be positive integers. If $m | n$, then $F_m | F_n$.*

Though we cannot find the original source for Lemma 2.4, there is a proof in [17], p. 64.

Lemma 2.4. *Let m, n be positive integers. Then, $\gcd(F_m, F_n) = F_{\gcd(m,n)}$.*

Lemma 2.5 follows from the definition of the Legendre symbol and Gauss' law of quadratic reciprocity.

Lemma 2.5. *Let p be prime. If $p \equiv \pm 1 (\mathrm{mod}\, 5)$, then $(\frac{p}{5}) = 1$. If $p \equiv \pm 2 (\mathrm{mod}\, 5)$, then $(\frac{p}{5}) = -1$. If p is odd, then $(\frac{5}{p}) = (\frac{p}{5})$.*

Lemma 2.6. *Let L be a positive integer and p be prime with $p | F_L$. Then, $\gcd(L, p - (\frac{p}{5})) > 2$.*

Proof. The statement is true for $p = 5$ because $5 | L$ if and only if $5 | F_L$. Let $p \neq 5$ be prime. From Lemmas 2.1, 2.2, and 2.5, we have $p | F_{p-(\frac{p}{5})}$. So, $p | \gcd(F_L, F_{p-(\frac{p}{5})})$. From Lemma 2.4, we have $p | F_{\gcd(L, p-(\frac{p}{5}))}$. Because no prime divides F_m for $m \leq 2$, we have $\gcd(L, p - (\frac{p}{5})) > 2$. □

Lemma 2.7. *Let L be a positive integer and p be prime with $p | F_L$. Assume $p \equiv \pm 1 (\mathrm{mod}\, L)$. Then, $p \equiv (\frac{p}{5}) (\mathrm{mod}\, L)$.*

Proof. Let $p \equiv \epsilon (\mathrm{mod}\, L)$, where $\epsilon \in \{-1, 1\}$. We have $p = kL + \epsilon$ for some $k \in \mathbb{Z}$. Thus, from Lemma 2.6, we have $2 < \gcd(L, p - (\frac{p}{5})) = \gcd(L, kL + \epsilon - (\frac{p}{5})) = \gcd(L, \epsilon - (\frac{p}{5}))$. Because $|\epsilon - (\frac{p}{5})| \leq 2$, we must have $\epsilon - (\frac{p}{5}) = 0$. □

In other words, consider the prime divisors p_i of F_L that satisfy $p_i \equiv \pm 1 (\mathrm{mod}\, L)$. Those p_i that satisfy $p_i \equiv 1 (\mathrm{mod}\, L)$ are those for which $p_i \equiv \pm 1 (\mathrm{mod}\, 5)$. Those that satisfy $p_i \equiv -1 (\mathrm{mod}\, L)$ are those for which $p_i \equiv \pm 2 (\mathrm{mod}\, 5)$. We are now ready to prove Theorem 1.1.

Proof. For each i, we have $p_i | F_L$ and $p_i \equiv \pm 1 (\mathrm{mod}\, L)$. Note that it is impossible for $5 | F_L$ and $5 \equiv \pm 1 (\mathrm{mod}\, L)$. So from Lemmas 2.5 and 2.7, for each i we have $p_i \equiv (\frac{5}{p_i}) (\mathrm{mod}\, L)$. Taking the product of both sides over all i gives $P \equiv (\frac{5}{P}) (\mathrm{mod}\, L)$. Thus, $L | (P - (\frac{5}{P}))$. From Lemma 2.3 we have $F_L | F_{P-(\frac{5}{P})}$. Because $P | F_L$, we get $P | F_{P-(\frac{5}{P})}$. □

Note that the construction described in Theorem 1.1 is related to, though not the same as, the construction in [4] of Fibonacci pseudoprimes.

Corollary 2.8. *Let L be an odd prime and p be a prime with $p | F_L$. Then, $p \equiv (\frac{p}{5}) (\mathrm{mod}\, L)$.*

Proof. From Lemma 2.6, because L is prime, we have $L | p - (\frac{p}{5})$. □

As explained in the introduction, we assume the following proposition is known. It can be proved independently of Theorem 1.1 and Corollary 2.8 using i) Lemma 2.3, ii) for L an odd prime, we have $F_L \equiv (\frac{5}{L}) (\mathrm{mod}\, L)$ (see [17], p. 60), and iii) for L odd, we have $L \equiv \pm 1 (\mathrm{mod}\, 5)$ implies $F_L \equiv \pm 1 (\mathrm{mod}\, 5)$ and $L \equiv \pm 2 (\mathrm{mod}\, 5)$ implies $F_L \equiv \pm 2 (\mathrm{mod}\, 5)$. We leave the construction of that proof to the reader.

Proposition 2.9. *Let L be prime and F_L be composite. Then, F_L is a Fibonacci pseudoprime.*

Proof. This result follows immediately from Theorem 1.1 and Corollary 2.8. □

Proposition 2.10. *Let L be a positive integer with $5 | L$. Let p be an odd prime with $p | F_L$ and $p \equiv \pm 1 (\mathrm{mod}\, L)$. Then, $p \equiv 1 (\mathrm{mod}\, L)$.*

Proof. From Lemma 2.7, we have $p \equiv (\frac{p}{5}) (\mathrm{mod}\, L)$. Because $5 | L$ and $p \equiv \pm 1 (\mathrm{mod}\, L)$, we have $p \equiv \pm 1 (\mathrm{mod}\, 5)$. The result follows from Lemma 2.5. □

3. The Search for a Baillie-PSW Pseudoprime

There is a $620 prize for a Baillie-PSW pseudoprime or a proof that none exists. A Baillie-PSW pseudoprime is an odd Fibonacci pseudoprime n that satisfies $n \equiv \pm 2 (\mathrm{mod}\, 5)$ and is also a base-2 pseudoprime. This problem was originally posed in [16]. Jan Feitsma and William Galway (see [7]) have computed all base-2 pseudoprimes up to 2^{64}. Sam Wagstaff has checked all of those to determine if there were any $620 winners and there were none (see [15]). The search is also described in [2], [4], [5], [12], [14], [16], and [19].

Our first search was inspired by Theorem 1.1. Fix a Fibonacci number F_L. For $j = -1, 1$ we let S_j be the set of odd prime divisors of F_L that are congruent to j modulo L. Recall, from Lemma 2.7, that the primes p_i in S_{-1} satisfy $p_i \equiv \pm 2 (\mathrm{mod}\, 5)$ and those in S_1 satisfy $p_i \equiv \pm 1 (\mathrm{mod}\, 5)$. When possible, we created products of at least two distinct primes from $S_{-1} \cup S_1$ such that the product contains an odd number of primes from S_{-1}. That way the product P satisfies $P \equiv \pm 2 (\mathrm{mod}\, 5)$. For example, for F_{258} we have $|S_{-1}| = 5$ and $|S_1| = 4$. Thus, we can create $\binom{5}{1} \cdot (2^4 - 1) + \binom{5}{3} \cdot 2^4 + \binom{5}{5} \cdot 2^4 = 251$ different products, each of which is an odd Fibonacci pseudoprime P that satisfies $P \equiv \pm 2 (\mathrm{mod}\, 5)$. From Proposition 2.10, if $5 | L$, then S_{-1} is empty and we can ignore such an L.

For our search, we used the complete and partial factorizations of Fibonacci numbers F_L into prime divisors for $1 \le L \le 9999$ found in [1] in Spring 2021. Using the construction described in the previous paragraph and these factorizations, we created approximately 2^{23} distinct odd Fibonacci pseudoprimes P that satisfy $P \equiv \pm 2 (\mathrm{mod}\, 5)$. We then checked each P to see if it is a base-2 pseudoprime, i.e., if $2^P \equiv 2 (\mathrm{mod}\, P)$. Alas, none were base-2 pseudoprimes. For programs and data, see [8].

Some of the Fibonacci pseudoprimes we created are huge. For example, because 9967 is prime and F_{9967} is composite (F_{9967} has been fully factored - see [1]), we see from Proposition 2.9 that F_{9967} is a Fibonacci pseudoprime. Note $F_{9967} \approx 2^{6918}$. If $P = \prod_{i=1}^{k} p_i$ is a huge Fibonacci pseudoprime, then using the relatively fast repeated squares algorithm to reduce $2^P (\mathrm{mod}\, P)$ can still be slow. Instead we note, by the Chinese Remainder Theorem, that $2^P \equiv 2 (\mathrm{mod}\, P)$ if and only if $2^P \equiv 2 (\mathrm{mod}\, p_i)$ for each i. We order the prime divisors of P as $p_1 < p_2 < \cdots < p_k$. First, we reduce $2^P (\mathrm{mod}\, p_1)$. If the remainder is not 2, as is usually the case, then we know P is not a base-2 pseudoprime. If the remainder is 2, we do the same computation for p_2, and so on. As soon as we get a remainder that is not 2, we can quit. If all k remainders are, in fact 2, then P is a base-2 pseudoprime (which never occurred for us).

We can speed up the computation of $2^P (\mathrm{mod}\, p_i)$ by noting that if $P \equiv r_i (\mathrm{mod}\, p_i - 1)$, with $0 \le r_i < p_i - 1$, then $2^P \equiv 2^{r_i} (\mathrm{mod}\, p_i)$, which is a consequence of Fermat's Little Theorem. Instead, we can reduce 2^{r_i} modulo p_i. To determine r_i, we can iteratively multiply together $((p_1 \cdot p_2) \cdot p_3) \ldots$, reducing modulo $p_i - 1$ after each multiplication. That way, the largest integer ever appearing in the algorithm is at most $p_{k-1} p_k$.

Our second search was inspired by Proposition 2.9. We checked increasing primes L up to 100000, which satisfy $L \equiv \pm 2 (\mathrm{mod}\, 5)$ (otherwise $F_L \equiv \pm 1 (\mathrm{mod}\, 5)$). For each such L, we used a pseudo-primality test to see which F_L were determined to be composite. If so, we then tested to see if F_L is a base-2 pseudoprime. Again, none were. For programs and data, see [8].

Acknowledgment

The authors are grateful to Carl Pomerance for challenging us to the $620 problem and useful conversations.

References

[1] Y. Amilin, S. Batalov, H. Bock, et al. (2021), Fibonacci and Lucas Factorizations, `http://mersennus.net/fibonacci/`
[2] R. Baillie and S. S. Wagtaff, Jr., *Lucas pseudoprimes*, Mathematics of Computation, **35** (1980), 1391–1417.
[3] R. D. Carmichael, *On the numerical factors of the arithmetic forms* $\alpha^n + \beta^n$, Annals of Mathematics, **15** (1913), 30–70.
[4] Z. Chen and J. Greene, *Some comments on Baillie-PSW pseudoprimes*, The Fibonacci Quarterly, **41.4** (2003), 334–344.
[5] R.E. Crandall and C. Pomerance, *Prime Numbers: A Computational Perspective*, (2nd ed.), Springer-Verlag, New York, 2005.
[6] A. DiPorto, P. Filipponi, and E. Montolivo, *On the generalized Fibonacci pseudoprimes*, The Fibonacci Quarterly, **28.4** (1990), 347–354.
[7] J. Feitsma and W. F. Galway (2013), Pseudoprimes, `http://www.janfeitsma.nl/math/psp2/index`.
[8] GitHub (2021), FibPseudoprime-SanitizedInputs, `https://github.com/ensj/FibPseudoprime-SanitizedInputs`.
[9] J. H. Halton, *On a general Fibonacci identity*, The Fibonacci Quarterly, **3.1** (1965), 31–43.
[10] E. Lehmer, *On the infinitude of Fibonacci pseudo-primes*, The Fibonacci Quarterly, **2.3** (1964), 229–230.
[11] E. Lucas, *Théorie des fonctions numériques simplement périodiques*, American Journal of Mathematics, **1** (1878), 184–240, 289–321.

[12] D. J. Monfre and D. Klyve, *Looking for Fibonacci base-2 pseudoprimes*, Missouri Journal of Mathematical Sciences, **24**, (2012), 116–123.
[13] E. A. Parberry, *On primes and pseudo-primes related to the Fibonacci sequence*, The Fibonacci Quarterly, **8.1** (1970), 49–60.
[14] C. Pomerance, *Are there counter-examples 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).
[15] C. Pomerance, *private communication.*
[16] C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr., *The pseudoprimes to* $25 \cdot 10^9$, Mathematics of Computation, **35** (1980), 1003–1026.
[17] P. Ribenboim, *The New Book of Prime Number Records*, Spring-Verlag, New York, 1996.
[18] A. Rotkiewicz, *Lucas and Frobenius pseudoprimes*, Annales Mathematicae Silesiane, **17** (2003), 17–39.
[19] A. Shallue and J. Webster, *Fast tabulation of challenge pseudoprimes*, The Open Book Series 2, ANTS XIII, Proceedings of the 13th Algorithmic Number Theory Symposium, eds. Renate Scheidler and Jonathan Sorenson, **2.1** (2019), 411–423.
[20] D. D. Wall, *Fibonacci series modulo m*, American Mathematical Monthly, **67** (1960), 525–532.

MSC2020: 11A51, 11B39, 11Y11

Department of Mathematics and Statistics, University of Minnesota Duluth, Duluth, MN 55812.
Email address: jgreene@d.umn.edu

Department of Mathematics and Computer Science, Santa Clara University, Santa Clara, CA 95053.
Email address: limjunhyun@gmail.com

Department of Mathematics and Computer Science, Santa Clara University, Santa Clara, CA 95053.
Email address: ssmash724@gmail.com

Department of Mathematics and Computer Science, Santa Clara University, Santa Clara, CA 95053.
Email address: eschaefer@scu.edu