A NEW PRIMALITY TEST USING FIBONNACI NUMBERS?

Abstract. In this paper, we ask whether a heuristic test for prime numbers can be derived from the Fibonacci numbers. The results below test for values up to F_{75} show that we might have a heuristic test for prime numbers akin to Fermat's Little Theorem.

Introduction

In early mathematics, it was thought that Mersenne Primes of the form $2^n - 1$ were prime when n is also prime. This certainly holds true for the first few values of n:

$$2^2 - 1 = 3$$
$$2^3 - 1 = 7$$
$$2^5 - 1 = 31$$
$$2^7 - 1 = 127.$$

However, it does not hold for all primes n. For example,

$$2^{11} - 1 = 2047 = 23.89.$$

In 1640, Fermat showed that it was not true of $n = 23$ and $n = 37$:

$$2^{23} - 1 = 8388607 = 47.178481$$
$$2^{37} - 1 = 137438953471 = 223.616318177.$$

In the same year Fermat proved that if p is a prime number, then for any integer a, the number $a^p - a$ is an integer multiple of p. This is known as Fermat's Little Theorem. So for the first few, where $a = 2$, we get:

$$2^2 - 2 = 2.1$$
$$2^3 - 2 = 3.2$$
$$2^5 - 2 = 5.6$$
$$2^7 - 2 = 7.18$$
$$2^{11} - 2 = 11.186$$
$$2^{13} - 2 = 13.630$$
$$2^{17} - 2 = 17.7710$$

All the results for prime exponents to infinity are divisible by the prime exponent that produced them. But if p is composite then the result is not divisible by p. It is therefore the basis for the so-called 'Fermat primality test' and is one of the fundamental results of elementary number theory.

Date: Sept 2019.
2010 *Mathematics Subject Classification.* Primary 11B39, 11A41.
Key words and phrases. Fibonnaci, Primes.

However, the converse is not true. In early China it was wrongly thought that a number, n, is prime if the expression $2^n - 2$ is a multiple of n. So $2^3 - 2$ is divisible by 3, $2^5 - 2$ is divisible by 5 and so on. But $2^{341} - 2$ is divisible by 341 (=11 x 31).

Fibonacci Numbers. Here we examine a similar text for primes using the Fibonacci sequence. The Fibonacci numbers are:

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34...$$

They are the sequence of numbers $F_n{}_{(n=1)}^{\infty}$ defined by the linear recurrence equation

$$F_n = F_{(n-1)} + F_{(n-2)}$$

where $F_0 = 0$ and $F_1 = F_2 = 1$.

In the following conjecture, we are not concerning ourselves directly with Fibonacci primes. A Fibonacci prime is a Fibonacci number F_n that is also a prime number, e.g. 2,3,5,13,89.... It is also known that every F_n that is prime must have a prime index n, with the exception of $F_4 = 3$. However, the converse is not true (i.e., not every prime index p gives a prime F_p), e.g. $F_{19} = 4181 = 37.113$.

Existing Fibonacci primality tests. A Fibonacci primality test already exists, but as I am aware, not for all primes. Lucas, and later Lehmer also explored using the Fibonacci sequence and more general Lucas sequences to test n for primality.[1] For example, if $p \equiv \pm 2 \pmod 5$, then $u_{p+1} \equiv 0 \pmod p$, where u_k denotes the kth Fibonacci number. This can be turned into a primality criterion for numbers $n \equiv \pm 2 \pmod 5$ provided you have the prime factorization of $n + 1$, or a large factored portion. For $n \not\equiv \pm 2 \pmod 5$ we can use other Lucas sequences.

This has led John Selfridge to conjecture that if p is an odd number, and $p \equiv \pm \pmod 5$, then p will be prime if both of the following hold:[2]

$$2^p - 1 \equiv 1 \pmod p,$$

$$f_{p+1} \equiv 0 \pmod p,$$

where f_k is the k^{th} Fibonacci number. The first condition is the Fermat primality test using base 2.

In general, if $p \equiv a \pmod{x^2+4}$, where a is a quadratic non-residue $\pmod{x^2+4}$ then p should be prime if the following conditions hold:

$$2^p - 1 \equiv 1 \pmod p,$$

$$f(x)_{p+1} \equiv 0 \pmod p,$$

then $f(x)k$ is the k-th Fibonacci polynomial at x.

[1]https://people.csail.mit.edu/vinodv/COURSES/MAT302-S13/pomerance.pdf
[2]https://en.wikipedia.org/wiki/Primality-testHeuristic-tests

Conjecture. Here we conjecture that (except for $p = 5$) if p is prime, then p will always divide $F_p + 1$ (if F_p terminates in the digits 3 or 7) or will divide $F_p - 1$ (if F_p terminates in the digits 1 or 9). The same will happen only for $2p$, where $2p$ will divide $F_{2p} \pm 1$ (under equivalent conditions). Stated alternatively, for all p, $F_p \equiv \pm 1 \pmod{p}$, $F_{2p} \equiv \pm 1 \pmod{2p}$. For all other composites, $F_n \not\equiv \pm 1 \pmod{n}$.

The table below gives the results up to $n = 75$. In the first column, n, the prime values of n are highlighted in bold; the second column is the Fibonacci sequence; the third and fourth rows are, respectively, the necessary calculations to 2 decimal places (integer results for p are marked in bold, and for $2p$ are marked [ ]*); the last column shows whether 1 was added or subtracted. Note that the only case for which this does not work is $n = 5$, $n = 10$.

n	F_n	$\frac{F_n+1}{n}$	$\frac{F_n-1}{n}$	$\equiv \pm 1 \pmod{p}$
1	1	2.00 (trivial)	0.00	-
2	1	**1.00**	0.00	+1
3	2	**1.00**	0.33	+1
4	3	[1.00]*	0.50	+1
5	5	1.20	0.80	-
6	8	1.50	1.17	-
7	13	**2.00**	1.71	+1
8	21	2.75	2.50	-
9	34	3.89	3.67	-
10	55	5.60	5.40	-
11	89	8.18	**8.00**	−1
12	144	12.08	11.92	-
13	233	**18.00**	17.85	+1
14	377	[27.00]*	26.86	-
15	610	40.73	40.60	-
16	987	61.75	61.63	-
17	1597	**94.00**	93.88	+1
18	2584	143.61	143.50	-
19	4181	220.11	**220.00**	−1
20	6765	338.30	338.20	-
21	10946	521.29	521.19	-
22	17711	805.09	[805.00]*	-
23	28657	**1246.00**	1245.91	+1
24	46368	1932.04	1931.96	-
25	75025	3001.04	3000.96	-
26	121393	[4669.00]*	4668.92	-
27	196418	7274.78	7274.70	-
28	317811	11350.43	11350.36	-
29	514229	17732.07	**17732.00**	−1
30	832040	27734.70	27734.63	-
31	1346269	43428.06	**43428.00**	−1

Continued on next page

Continued from previous page

n	F_n	$\frac{F_n+1}{n}$	$\frac{F_n-1}{n}$	$\equiv \pm 1 \pmod{p}$
32	2178309	68072.19	68072.13	-
33	3524578	106805.42	106805.36	-
34	5702887	[167732.00]*	167731.94	-
35	9227465	263641.89	263641.83	-
36	14930352	414732.03	414731.97	-
37	24157817	**652914.00**	652913.95	+1
38	39088169	1028636.05	[1028636.00]*	-
39	63245986	1621691.97	1621691.92	-
40	102334155	2558353.90	2558353.85	-
41	165580141	4038540.05	**4038540.00**	−1
42	267914296	6378911.83	6378911.79	-
43	433494437	**10081266.00**	10081265.95	+1
44	701408733	15941107.59	15941107.55	-
45	1134903170	25220070.47	25220070.42	-
46	1836311903	[39919824.00]*	39919823.96	-
47	2971215073	**63217342.00**	63217341.96	+1
48	4807526976	100156812.02	100156811.98	-
49	7778742049	158749837.76	158749837.71	-
50	12586269025	251725380.52	251725380.48	-
51	20365011074	399313942.65	399313942.61	-
52	32951280099	633678463.46	633678463.42	-
53	53316291173	**1005967758.00**	1005967757.96	+1
54	86267571272	1597547616.17	1597547616.13	-
55	139583862445	2537888408.11	2537888408.07	-
56	225851433717	4033061316.39	4033061316.36	-
57	365435296162	6411145546.72	6411145546.68	-
58	591286729879	10194598791.03	[10194598791.00]*	-
59	956722026041	16215627560.03	**16215627560.00**	−1
60	1548008755920	25800145932.02	25800145931.98	-
61	2504730781961	41061160360.03	**41061160360.00**	−1
62	4052739537881	65366766740.03	[65366766740.00]*	-
63	6557470319842	104086830473.70	104086830473.67	-
64	10610209857723	165784529026.94	165784529026.91	-
65	17167680177565	264118156577.94	264118156577.91	-
66	27777890035288	420877121746.80	420877121746.77	-
67	44945570212853	**670829406162.00**	670829406161.97	+1
68	72723460248141	1069462650707.97	1069462650707.94	-
69	117669030460994	1705348267550.65	1705348267550.62	-
70	190392490709135	2719892724416.23	2719892724416.20	-
71	308061521170129	4338894664368.03	**4338894664368.00**	−1
72	498454011879264	6922972387212.01	6922972387211.99	-
73	806515533049393	**11048157986978.00**	11048157986978.00	+1
74	1304969544928660	[17634723580117.00]*	17634723580117.00	-

Continued on next page

Continued from previous page

n	F_n	$\frac{F_n+1}{n}$	$\frac{F_n-1}{n}$	$\equiv \pm 1 \pmod{p}$
75	2111485077978050	28153134373040.70	28153134373040.70	-

Table 1: It ends from the previous page.

Interestingly, the composite 341, a pseudoprime for Fermat's Little Theorem, properly follows the algorithm:

$F_{341} = 82281144336295989585340713815384441479925901307982452831610787275979941$

And indeed,

$$\frac{F_{341}-1}{341} =$$

$$2412936784055600867605299525377842858648853410791274276586826606 33372.2580\\ 645161290322580645161290322580645161290322580645161290323.$$

...a fraction, as expected.

But the critical question is: are there any pseudoprimes using this test?

References

1. http://mathworld.wolfram.com/FibonacciNumber.html. Last accessed 21.09.19.
2. http://www.maths.surrey.ac.uk/hosted-sites/R.Knott/Fibonacci/fibtable301.html
3. http://www.maths.surrey.ac.uk/hosted-sites/R.Knott/contactron.htmlsection1.1
4. https://en.wikipedia.org/wiki/Primality-testHeuristic-tests
5. https://people.csail.mit.edu/vinodv/COURSES/MAT302-S13/pomerance.pdf

The Rectory, Village Road, Waverton, Chester Ch3 7QN, UK
Email address: julianbeauchamp47@gmail.com