A CONJECTURE ON THE SUFFIX OF THE FIRST FIBONACCI NUMBER DIVISIBLE BY A GIVEN PRIME*

by

Anirban DasGupta
Purdue University

Technical Report #99-16

Department of Statistics
Purdue University
West Lafayette, IN USA

August 1999

*

A CONJECTURE ON THE SUFFIX OF THE FIRST FIBONACCI NUMBER DIVISIBLE BY A GIVEN PRIME*

by

Anirban DasGupta
Purdue University

Abstract

Two well known problems on the Fibonacci sequence ask if there are infinitely many primes among the Fibonacci numbers and what is the suffix $n(p)$ of the first Fibonacci number divisible by a given prime number p. It is known that at least one among the first $p+1$ Fibonacci numbers is always divisible by a prime p, although the exact number $f(p)$ does not have a general formula. It is known that $(p-(5/p))/n(p)$ is an integer, with $(5/p)$ denoting the Legendre symbol, although the limsup of the sequence $(p-(5/p))/n(p)$ is ∞.

We present some computations that strongly suggest that asymptotically the median of $n(p)/p$ is $1/2$ and the median of $f(p)$ is 2. Actually, the first fact would analytically imply the second. The sequences $n(p)$ and $f(p)$ show significant local oscillation, but the probability distributions show consistency and stability in a number of ways. For instance, the probability that $n(p)$ is $(p+1)/2$ remains stable when the number of primes in consideration is increased.

Asymptotically, $n(p)/p$ lives on the set $\{1, 1/2, 1/3, \ldots\}$. This also suggests a preliminary but useful test to check if a given Fibonacci number is likely to be a prime. In 24 test cases, the test worked in 22 cases.

Exhaustive lists of both $n(p)$ and $f(p)$ are provided at the end for the first 600 primes.

*Research supported by a grant from The National Security Agency.

1. Introduction

The Fibonacci sequence F_n defined by the recurrence relation $F_{n+2} = F_{n+1} + F_n, F_1 = F_2 = 1$ has a very special status in mathematics and number theory. The Fibonacci sequence shows up in many areas of mathematics, for example, continued fractions, primality testing, probabilities on the symmetric group, linear algebra, and many more. See Lucas (1878), Vorob'ev (1961), Hogatt (1969), Philippou et al (1984), Tomescu (1985), for instance.

There are two problems about the Fibonacci sequence that may duly be described as being famous. One is to decide if there are infinitely many primes among the Fibonacci numbers. The other is to give a formula for the index of the Fibonacci number whose primitive prime factor is a given prime number p. In other words, it is known that any prime number p divides one or more members of the Fibonacci sequence and in fact it is also known that p divides at least one of the first $p+1$ Fibonacci numbers. The question is what is the suffix of the first one among the Fibonacci numbers that has p as a prime factor?

In the sequel, for any given prime p, we will denote by $n(p)$ the index of the first Fibonacci number with p as a prime factor, and we will denote by $f(p)$ the number of Fibonacci numbers among the first $p+1$ Fibonacci numbers that are divisible by p.

It follows from elementary properties of the Fibonacci sequence that $f(p)$ has a formula in terms of $n(p)$. Indeed, for any m, n, F_m divides F_n if and only if m divides n. And so if F_n is divisible by p, so would be F_{kn} for $k > 1$. Since we are interested in only the first $p+1$ Fibonacci numbers, it follows that $f(p) = [(p+1)/n(p)]$, the integer part of $(p+1)/n(p)$.

As regards $n(p)$ itself, we know that if $\psi(p)$ denotes $p - (5/p)$ where $(./.)$ denotes the Legendre symbol, then $\psi(p)/n(p)$ is an integer. Since $\psi(p)$ is $p \pm 1$, this means that asymptotically, $p/n(p)$ would take approximately integral values. Jarden (1958) had shown that $\limsup \psi(p)/n(p)$ is ∞; as a consequence, asymptotically, $p/n(p)$ takes approximately integral values, but if we look at a large number of primes, we will see large integral values in the range of $p/n(p)$, and equivalently, small numbers in the range of $n(p)/p$.

Although everything here is deterministic, one could introduce randomness in a natural sort of way. For any given integer $N \geq 1$, one could look at the sequence $n(p)$ and $f(p)$ for the first N prime numbers, and study their statistical properties if a uniform distribution is assigned to these N prime numbers. Then one could ask what happens when $N --> \infty$. This is a standard approach in probabilistic number theory; see for instance Elliott (1979).

In this note, we present some computation which very strongly suggests that the asymptotic median of $n(p)/p$ is $1/2$, and the asymptotic median of $f(p)$ is 2. Indeed, for a range of values of N, the medians stay consistently close to these asymptotic values. Although an analytical proof is not available, almost certainly the asymptotic median of $f(p)$ is 2. The probability distributions of $n(p)/p$ and $f(p)$ themselves show some other interesting phenomena. This is discussed in more detail in Section 2. Since asymptotically $n(p)/p$ lives on the integer reciprocals $1/i, i = 1, 2, 3, \ldots$, verifying whether a given Fibonacci number (of a large index n) is likely to be a prime can benefit from verifying whether F_n/n is very close to being an integer. One could use such an initial test before actually verifying the primality of a large Fibonacci number. In fact, in some numerical verification, this initial test worked out quite nicely. As an example, for F_{2971}, which has 621 digits and is known to be a prime number, the difference of $F_{2971}/2971$ from its nearest integer was only .00034; on the other hand, for F_{2970}, which is composite, the difference of $F_{2970}/2970$ from its nearest integer is .14815.

2. The Computation

For the sequence $n(p)$, the four values $(p-1)/2, (p+1)/2, p-1$, and $p+1$ happen to be special ones; frequently, $n(p)$ is one of these four values. For $N = 600$, i.e., if we take the first 600 primes, we evaluated $n(p)$ and $f(p)$ exhaustively. For $N = 2500$, we evaluated $n(p)$ and $f(p)$ for a random sample of 500 primes. It was a bit surprising that even when only 200 primes were considered, the median value of $n(p)/p$ was extremely close to $1/2$, and for larger N, the median remained extremely close to $1/2$ consistently. However, the distribution of $n(p)/p$ has a long right tail, causing the mean to be hovering around .6. Likewise the mean of $f(p)$ was considerably larger than 2, and was increasing with N. Moreover, $f(p)$ had such large oscillations, that its correlation with p seemed to be converging to zero. First in Table 1 and Table 2, we summarize these few findings.

Table 1

	$N = 200$	$N = 600$	$N = 2500$
$P(n(p) = p-1)$	.175	.18	.18
$P(n(p) = p+1)$	.21	.193	.194
$P(n(p) = \frac{p-1}{2})$	.1	.093	.114
$P(n(p) = \frac{p+1}{2})$	.21	.208	.194
Median of $\frac{n(p)}{p}$	.5009	.5002	.5004
$E(\frac{n(p)}{p})$	.6058	.5914	.5879
Correlation$(p, n(p))$	.6255	.6736	.6964

Table 2

	$N = 200$	$N = 600$	$N = 2500$
$P(f(p) = 1)$	.39	.375	.376
$P(f(p) = 2)$	.31	.302	.308
Median of $f(p)$	2	2	2
$E(f(p))$	3.3050	4.442	5.314
Correlation$(p, f(p))$	.1754	.0727	$-.0358$

Figure 1, 2, and 3 give the scatterplot for $(p, n(p))$ for $N = 200, 600$, and 2500 respectively. The plots immediately reveal concentrations around the lines $n(p) = p/2$ and $n(p) = p$. One can see from the plots that the relationship is not monotone, but there is a general monotonic trend. The scatterplot for $(p, f(p))$ is given in Figure 4 for the case $N = 2500$.

Of course, for any given N, the values of $n(p)/p$ are not exactly equal to the values $1/i, i = 1, 2, \ldots$. But, even for rather small N, they are almost so. For $N = 2500$, Table 3 gives the relative frequencies of the values $1/i, i = 1, 2, \ldots, 12$, among the values $n(p)/p$. The first three values $1, 1/2$ and $1/3$ share more than $3/4$ of the probability. There is an interesting local peak at the values $1/6$ and $1/12$.

Table 3

$P(\frac{n(p)}{p} = \frac{1}{i})$ for $N = 2500$

i	1	2	3	4	5	6	7	8	9	10	11	12
$P(\frac{n(p)}{p} = \frac{1}{i})$	.376	.308	.074	.066	.01	.034	.008	.008	.01	.012	.004	.016

Table 4 and Table 5 are at the end of this note. Table 4 gives a complete list of $n(p)$ for the first 600 primes, and Table 5 gives a complete list of $f(p)$ for the first 600 primes. Each list demonstrates the very significant local oscillation in $n(p)$ and $f(p)$ as p changes.

2.1 Primality Testing for Fibonacci Numbers

The general purpose algorithms for primality testing would not be very efficient for testing a Fibonacci number of large suffix for primality. There are certain specialized algorithms, however. Still, in some situations, it could be useful to have a quick and dirty initial test for primality. We saw in the previous section that asymptotically, the sequence $n(p)/p$ lives on the set $\{1, 1/2, 1/3, \ldots\}$. Suppose now that we take p to be a certain

Fibonacci number F_n which happens to be a prime. So for this $p, n(p)$ is n. Heuristically, therefore, $n(p)/p = n/F_n$ should be approximately equal to $1/i$ for some integer i, and F_n/n should be approximately equal to an integer i. So for a general Fibonacci number F_k, one could compute F_k/k to see how far it is from its nearest integer. If it is not close, F_k is likely to be not a prime. Table 6 and Table 7 illustrate how well this heuristic test works. In Table 6 all the Fibonacci numbers are primes; in Table 7, none of the Fibonacci numbers is a prime. See Brillhart (1963) and Ribenboim (1991). The test appears to work well if the suffix k is about 100 or larger.

Table 6

k	$\lvert \frac{Fk}{k} -$ integer closest to $\frac{F_k}{k} \rvert$
43	.02325
47	.02128
83	.01205
131	.00763
137	.00730
359	.00279
431	.00232
449	.00222
509	.00196
569	.00176
571	.00175
2971	.00034

Table 7

k	$\mid \frac{F_k}{k} -$ integer closest to $\frac{F_k}{k} \mid$
136	.15441
138	.05797
358	.00279
430	.12791
448	.29688
450	.22222
508	.49409
510	.21569
568	.28697
570	.38600
572	.00175
2970	.14815

REFERENCES

Brillhart, J., (1963). Some miscellaneous factorizations, *Math. Comp.*, **17**, 447–450.

Elliott, P.D.T.A. (1979). Probabilistic Number Theory II, Central Limit Theorems, Springer–Verlag, New York.

Hogatt, V.E., Jr. (1969). Fibonacci and Lucas Numbers, Houghton Mifflin Co., Boston.

Jarden, D. (1958). Recurring Sequences (Third Edition), Fibonacci Association, San Jose, CA.

Lucas, E. (1878). Theorie des fonctions numeriques simplement periodiques, *Amer. J. Math*, **1**, 184–240, 289–321.

Philippou, A.N., Bergum, G.E., and Horadam, A.F., Eds. (1984). Fibonacci Numbers and Their Applications, D. Reidel Publishing Co., Doradrecht, Netherlands.

Ribenboim, P. (1991). The Little Book of Big Primes, Springer–Verlag, New York.

Tomescu, I. (1985). Problems in Combinatorics and Graph Theory (Translated by Melter, R.A.), John Wiley, New York.