A RESULT ABOUT THE PRIMES DIVIDING FIBONACCI NUMBERS

Mansur S. Boase
Trinity College, Cambridge CB2 1TQ, England
(Submitted March 1998-Final Revision February 2001)

1. INTRODUCTION

The following theorem arose from my correspondence with Dr. Peter Neumann of Queen's College, Oxford, concerning the number of ways of writing an integer of the form $F_{n_1}F_{n_2}\dots F_{n_r}$ as a sum of two squares.

Theorem 1.1: If $m \geq 3$, then with the exception of $m = 6$ and $m = 12$, F_m is divisible by some prime p which does not divide any F_k, $k < m$.

Theorem 1.1 is similar to a theorem proved by K. Zsigmondy in 1892 (see [4]), which states that, for any natural number a and any m, there is a prime that divides $a^m - 1$ but does not divide $a^k - 1$ for $k < m$ with a small number of explicitly stated exceptions. A summary of Zsigmondy's article can be found in [2, Vol. 1, p. 195]. Since the arithmetic behavior of the sequence of Fibonacci numbers F_n is very similar to that of the sequences $a^n - b^n$ (for fixed a and b), Theorem 1.1 can be regarded as an analog of Zsigmondy's theorem for the Fibonacci sequence.

2. PRELIMINARY LEMMAS

This section includes a few lemmas that are required for the proof of Theorem 1.1.

Lemma 2.1: Let m, n be positive integers and let (a, b) denote the highest common factor of a and b. Then

$$\left(\frac{F_{mn}}{F_n}, F_n\right) \Bigg| \, m.$$

Proof: First, we prove by induction on m that

$$\frac{F_{mn}}{F_n} \equiv m(F_{n-1})^{m-1} \pmod{F_n}.$$

The result holds for $m = 1$. Suppose the result holds for $m = k$. Then

$$\frac{F_{kn}}{F_n} \equiv k(F_{n-1})^{k-1} \pmod{F_n}.$$

Now

$$F_{m+n+1} = F_m F_n + F_{m+1}F_{n+1} \quad \text{(see [1] or [3])}, \tag{1}$$

so $F_{(k+1)n} = F_{kn+(n-1)+1} = F_{kn}F_{n-1} + F_{kn+1}F_n$. Therefore,

$$\frac{F_{(k+1)n}}{F_n} = \frac{F_{kn}}{F_n}F_{n-1} + F_{kn+1} \equiv k(F_{n-1})^{k-1}F_{n-1} + F_{kn+1} \pmod{F_n}$$
$$\equiv k(F_{n-1})^k + F_{kn+1} \pmod{F_n}.$$

Using (1) again,

$$F_{kn+1} = F_{(k-1)n}F_n + F_{(k-1)n+1}F_{n+1} \equiv F_{(k-1)n+1}F_{n+1} \pmod{F_n}$$
$$\equiv F_{(k-1)n+1}F_{n-1} \pmod{F_n}.$$

Similarly, $F_{(k-1)n+1} \equiv F_{(k-2)n+1}F_{n-1} \pmod{F_n}$ giving us

$$F_{kn+1} \equiv F_{(k-1)n+1}F_{n-1} \equiv F_{(k-2)n+1}(F_{n-1})^2 \equiv \cdots \equiv (F_{n-1})^k \pmod{F_n}.$$

Therefore,

$$\frac{F_{(k+1)n}}{F_n} \equiv k(F_{n-1})^k + (F_{n-1})^k \equiv (k+1)(F_{n-1})^k \pmod{F_n}.$$

This completes the inductive step.

Let us define

$$d = \left(\frac{F_{mn}}{F_n}, F_n\right) = (m(F_{n-1})^{m-1} + tF_n, F_n),$$

where t is some integer. Then we have $d \mid F_n$ and $d \mid m(F_{n-1})^{m-1}$. However, $(F_n, F_{n-1}) = 1$, so d divides m and the lemma is proved. □

Lemma 2.2:

$$p_1^{\alpha_1}p_2^{\alpha_2}\dots p_n^{\alpha_n} = \frac{\displaystyle\prod_{k\text{ odd}} \frac{p_1^{\alpha_1}p_2^{\alpha_2}\dots p_n^{\alpha_n}}{p_{i_1}p_{i_2}\cdots p_{i_k}}}{\displaystyle\prod_{k\text{ even}} \frac{p_1^{\alpha_1}p_2^{\alpha_2}\dots p_n^{\alpha_n}}{p_{i_1}p_{i_2}\cdots p_{i_k}}},$$

where the numerator is the product of all numbers of the form $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_n^{\alpha_n}$ divided by an odd number of distinct primes and the denominator is the product of all numbers of the form $p_1^{\alpha_1}p_2^{\alpha_2}\dots p_n^{\alpha_n}$ divided by an even nonzero number of distinct primes.

Proof: The exponent of p_r on the left-hand side is α_r. The exponent of p_r in the numerator of the right-hand side is

$$\sum_{k\text{ odd}} \left(\alpha_r\binom{n}{k} - \binom{n-1}{k-1}\right),$$

as there are $\binom{n}{k}$ ways of choosing $i_1, \dots, i_k$ and, if $i_s = r$ for some s, there are $\binom{n-1}{k-1}$ ways of choosing the other i_j. Similarly, the exponent of p_r in the denominator of the right-hand side is

$$\sum_{k\text{ even}} \left(\alpha_r\binom{n}{k} - \binom{n-1}{k-1}\right),$$

so the exponent of p_r on the right-hand side is

$$\alpha_r\left(\binom{n}{1} - \binom{n}{2} + \binom{n}{3} - \cdots + (-1)^n\binom{n}{n}\right) - \left(1 - \binom{n-1}{1} + \binom{n-1}{2} - \cdots + (-1)^{n-1}\binom{n-1}{n-1}\right)$$
$$= \alpha_r(1-(1-1)^n) - (1-1)^{n-1} = \alpha_r$$

as required. □

Lemma 2.3: If $0 < a < 1$, then $\prod_{n=1}^{\infty}(1-a^n) > (1-a)^{\frac{1}{1-a}}$.

Proof: Equivalently, we must prove that

$$\sum_{n=1}^{\infty}\ln(1-a^n) > \frac{\ln(1-a)}{1-a}.$$

If $|x|<1$, then the Taylor series expansion for $\ln x$ about $x=1$ is $\ln(1+x) = x-\frac{x^2}{2}+\frac{x^3}{3}-\cdots$. Thus,

$$\ln(1-a^n) = -\left(a^n+\frac{a^{2n}}{2}+\frac{a^{3n}}{3}+\cdots\right).$$

Therefore,

$$\sum_{n=1}^{\infty}\ln(1-a^n) = -\sum_{k=1}^{\infty}\frac{1}{k}(a^k+a^{2k}+a^{3k}+\cdots)$$

$$= -\sum_{k=1}^{\infty}\frac{1}{k}\left(\frac{a^k}{1-a^k}\right) > -\sum_{k=1}^{\infty}\frac{1}{k}\left(\frac{a^k}{1-a}\right) = \frac{\ln(1-a)}{1-a}. \quad \square$$

Lemma 2.4: If $a=(\sqrt{5}-1)/(\sqrt{5}+1)$, then

$$\prod_{\substack{n \text{ odd}\\ n\geq 1}}(1-a^n) \Big/ \prod_{\substack{n \text{ even}\\ n\geq 2}}(1-a^n) < 2.$$

Proof: Note that $1-x^2<1$ and so, for $x<1$, we have $1+x<(1-x)^{-1}$. Thus,

$$\prod_{\substack{n \text{ odd}\\ n\geq 1}}(1-a^n) \Big/ \prod_{\substack{n \text{ even}\\ n\geq 2}}(1-a^n) < (1+a)\Big/\prod_{n=2}^{\infty}(1-a^n)$$

$$= (1-a^2)\Big/\prod_{n=1}^{\infty}(1-a^n) < (1-a^2)(1-a)^{\frac{-1}{1-a}} < 2,$$

where the penultimate inequality follows from Lemma 2.3, and the final inequality holds for the value of a given. $\square$

Lemma 2.5: If $m=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_n^{\alpha_n}$, then the only solutions m, $m\geq 3$, to the inequality

$$f(m) = \left(\frac{1+\sqrt{5}}{2}\right)^{(p_1^{\alpha_1}-p_1^{\alpha_1-1})\ldots(p_n^{\alpha_n}-p_n^{\alpha_n-1})} \leq 2p_1\ldots p_n = g(m) \tag{2}$$

are $m=3, 4, 5, 6, 10, 12, 14$, and 30.

We first prove the following three easy facts:

(i) If $f(m)>Cg(m)$, $C>1$, and m' is formed from m by replacing p_i in the prime factorization of m by q_i, where $q_i>p_i$ and $q_i\neq p_k$ for any k, then $f(m')>Cg(m')$.

(ii) If $f(m)>g(m)$ and p is an odd prime, then $f(pm)>g(pm)$.

(iii) If $f(m)>g(m)$ and m is even, then $f(2m)>g(2m)$. If $f(m)>2g(m)$ and m is odd, then $f(2m)>g(2m)$.

Proof of (i): $f(m)>Cg(m)\geq 4C$ so, in particular, $f(m)>\exp(1)$. Now

$$q_i>p_i \Rightarrow q_ip_i-p_i>q_ip_i-q_i \Rightarrow \frac{q_i-1}{p_i-1}>\frac{q_i}{p_i},$$

so

$$f(m') \geq f(m)^{\frac{q_i-1}{p_i-1}} > f(m)^{\frac{q_i}{p_i}} = f(m)(f(m))^{\frac{q_i}{p_i}-1} > f(m)\exp\left(\frac{q_i}{p_i}-1\right).$$

Since $\exp(x-1) > x$ for $x > 1$, we have

$$f(m') > \left(\frac{q_i}{p_i}\right)f(m) > C\left(\frac{q_i}{p_i}\right)g(m) = Cg(m').$$

Proof of (ii): Note that $p > 2$ and $g(m) \geq 4$ so

$$f(pm) \geq f(m)^{p-1} > g(m)^{p-1} \geq 4^{p-2}g(m) > pg(m) \geq g(pm).$$

Proof of (iii): If m is even and $f(m) > g(m)$, then $f(2m) > f(m) > g(m) = g(2m)$. If m is odd and $f(m) > 2g(m)$, then $f(2m) = f(m) > 2g(m) = g(2m)$.

Proof of Lemma 2.5: We call m "good" if $f(m) > 2g(m)$ or if m is even and $f(m) > g(m)$. Note that, by (ii) and (iii), if m is good, then no multiple of m may satisfy inequality (2).

Standard calculations show that $m = 11$ is good. It then follows from (i) that every prime greater than 11 is good, so any solution m of (2) must only have 2, 3, 5, and 7 as prime divisors.

It is easy to show that $m = 3^2$ and $m = (3)(7)$ are good. So, by (i), except for $m = (3)(5)$, $m = p_i^2$ and $m = p_ip_j$ are good for odd primes p_i, p_j. Hence, the only odd numbers whose multiples may satisfy inequality (2) are 3, 5, 7, and 15.

Now $m = 2^3$ is good, as is $m = 2^2(5)$. Thus, $m = 2^2(p_i)$ is good for odd primes p_i, $p_i \geq 5$. Therefore, the only possible solutions to inequality (2) are 2, 3, 5, 7, (3)(5), (2)(3), (2)(5), (2)(7), (2)(3)(5), 2^2, and $2^2(3)$. Of these, 7 and (3)(5) are not solutions and $2 < 3$, so we obtain the list as stated in the lemma. □

3. PROOF OF THE MAIN THEOREM

Suppose we choose a Fibonacci number F_m, with $m \geq 3$ and $m = p_1^{\alpha_1}p_2^{\alpha_2}\dots p_n^{\alpha_n}$, such that all prime factors of F_m divide some previous Fibonacci number.

Then every prime dividing F_m must divide one of $F_{m[1]}, F_{m[2]}, \dots, F_{m[n]}$, where $m[i] = m/p_i$, making use of the well-known fact that $(F_m, F_n) = F_{(m,n)}$. Now $F_m \leq p_1p_2\cdots p_nF_{m[1]}F_{m[2]}\cdots F_{m[n]}$, for the left-hand side divides the right-hand side, using Lemma 2.1. However, some of the factors of F_m are being double counted, such as $F_{p_1^{\alpha_1-1}p_2^{\alpha_2-1}\dots p_n^{\alpha_n}}$, which divides both $F_{m[1]}$ and $F_{m[2]}$.

To remove repeats, the same Inclusion-Exclusion Principle idea of Lemma 2.2 can be used. This gives

$$F_m \leq p_1p_1\cdots p_n\frac{\prod_{k\text{ odd}} F_{m[i_1,i_2,\dots,i_k]}}{\prod_{k\text{ even}} F_{m[i_1,i_2,\dots,i_k]}}, \tag{3}$$

where $m[i_1, i_2, \dots, i_k] = m/p_{i_1}p_{i_2}\cdots p_{i_k}$ and the i_j are all distinct. In fact, the left-hand side divides the right-hand side, but the inequality is sufficient for our purposes.

It is now necessary to simplify (3) to obtain a weaker inequality that is easier to handle.

Multiplying by the denominator in (3),

$$\prod_{k\text{ even}} F_{m[i_1,i_2,\dots,i_k]} \leq p_1p_2\cdots p_n\prod_{k\text{ odd}} F_{m[i_1,i_2,\dots,i_k]}, \tag{4}$$

where we have absorbed F_m into the product on the left-hand side.

Let us define F_n' to equal

$$\frac{1}{\sqrt{5}}\left(\frac{1+\sqrt{5}}{2}\right)^n.$$

By Binet's formula,

$$F_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right) \quad \text{and} \quad -1 < \frac{1-\sqrt{5}}{2} < 0,$$

so, as $n \to \infty$, $F_n \to F_n'$. Furthermore, $F_n > F_n'$ for n odd and $F_n < F_n'$ for n even.

All the Fibonacci numbers on the left-hand side of (4) are of the form $F_{m/k}$, k a product of an even number of distinct primes, and they are all distinct since, if $F_{m/k} = F_{m/k'}$, then $k = k'$ or m/k and m/k' are 1 and 2 in some order, contradicting the fact that k and k' are both products of an even number of distinct primes. Let us define γ_1 to equal

$$\prod_{n \text{ even}} \left(\frac{F_n}{F_n'}\right),$$

where the product is taken over all even integers n. The left-hand side of (4) would therefore be made even smaller if all the F_n in it were replaced by F_n' and the result were multiplied by γ_1. Similarly, the right-hand side of (4) would be made even larger if all the F_n in it were replaced by F_n' and the result were multiplied by γ_2, where γ_2 is equal to

$$\prod_{n \text{ odd}} \left(\frac{F_n}{F_n'}\right).$$

Thus, if we define $\varepsilon = \gamma_2/\gamma_1$, we obtain from (4) the weaker inequality,

$$\prod_{k \text{ even}, \geq 0} F'_{m[i_1, i_2, \ldots, i_k]} \leq \varepsilon p_1 p_2 \ldots p_n \prod_{k \text{ odd}} F'_{m[i_1, i_2, \ldots, i_k]}. \tag{5}$$

The number of terms in the product on the left-hand side of (5) is $1 + \binom{n}{2} + \binom{n}{4} + \cdots$ and on the right-hand side is $\binom{n}{1} + \binom{n}{3} + \binom{n}{5} + \cdots$, and these numbers are equal as their difference is $(1-1)^n = 0$. Therefore, the $1/\sqrt{5}$ factors of F_n' will cancel on both sides, leaving

$$\left[\left(\frac{1+\sqrt{5}}{2}\right)^m\right]^{(1-\frac{1}{p_1})(1-\frac{1}{p_2})\cdots(1-\frac{1}{p_n})} \leq \varepsilon p_1 p_2 \ldots p_n,$$

on rearranging. Since $m = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_n^{\alpha_n}$, this simplifies to give

$$\left(\frac{1+\sqrt{5}}{2}\right)^{(p_1^{\alpha_1} - p_1^{\alpha_1 - 1})\cdots(p_n^{\alpha_n} - p_n^{\alpha_n - 1})} \leq \varepsilon p_1 p_2 \ldots p_n. \tag{6}$$

Now, setting $a = (\sqrt{5}-1)/(\sqrt{5}+1)$,

$$\gamma_1 = \prod_{n \text{ even}} \left(\frac{F_n}{F_n'}\right) = \prod_{n \text{ even}} \left(\frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{(1+\sqrt{5})^n}\right) = \prod_{n \text{ even}} (1 - a^n).$$

Similarly,

$$\gamma_2 = \prod_{n \text{ odd}} \left(\frac{F_n}{F_n'}\right) = \prod_{n \text{ odd}} \left(\frac{(1+\sqrt{5})^n - (1-\sqrt{5})^n}{(1+\sqrt{5})^n}\right) = \prod_{n \text{ odd}} (1 - a^n).$$

Therefore, by Lemma 2.4,

$$\varepsilon = \gamma_2 / \gamma_1 < 2.$$

Now Lemma 2.5 gives us a list of possible m which may satisfy inequality (6). Thus, it only remains for us to check which of these m give rise to F_m, all of whose prime factors divide some previous Fibonacci number. The possible solutions, m, to (6), with $m \geq 3$, are 3, 4, 5, 6, 10, 12, 14, and 30.

Note that $2|F_3$, $3|F_4$, $5|F_5$, $11|F_{10}$, $29|F_{14}$, and $31|F_{30}$ and the respective primes do not divide any previous Fibonacci numbers. Thus, the only exceptions to the result are $F_6 = 8$ and $F_{12} = 144$. Therefore, Theorem 1.1 is proved. □

A similar result can also be proved for the Lucas numbers.

Corollary 3.1: If $m \geq 2$, then, with the exception of $m = 3$ and $m = 6$, L_m is divisible by some prime p that does not divide any L_k, $0 \leq k < m$.

Proof: Suppose $m \geq 2$ and m does not equal 3 or 6. Then, since $2m \geq 3$ and $2m$ does not equal 6 or 12, Theorem 1.1 implies the existence of a prime p such that p divides F_{2m}, but does not divide any smaller Fibonacci number. Now $F_{2m} = F_m L_m$ (see [3]), so p must divide L_m. We claim that p does not divide any L_k for $k < m$, for $p|L_k$ would imply $p|F_{2k}$, and since $2k < 2m$, this contradicts our choice of p. Hence, the corollary. □

We end with the following conjecture for the general Fibonacci-type sequence.

Conjecture 3.2: Suppose that K_1 and K_2 are positive integers and that K_n is defined recursively for $n \geq 3$ by $K_n = K_{n-1} + K_{n-2}$. Then, for all sufficiently large m, there exists a prime p that divides K_m but does not divide any K_r, $r < m$.

ACKNOWLEDGMENTS

I am very grateful to Dr. Peter Neumann for all his help, to Professors Murray Klamkin and Michael Bradley for their encouragement, and to the anonymous referee for detailed comments and corrections that helped to improve this paper significantly.

REFERENCES

1. M. S. Boase. "An Identity for Fibonacci Numbers." *Math. Spectrum* **30.2** (1997/98):42-43.
2. L. E. Dickson. *History of the Theory of Numbers*. New York: Chelsea, 1952.
3. V. E. Hoggatt, Jr. *Fibonacci and Lucas Numbers*. Santa Clara, Calif.: The Fibonacci Association, 1972.
4. K. Zsigmondy. "Zur Theorie der Potenzreste." *Monatshefte Math. Phys.* **3** (1892):265-84.

AMS Classification Numbers: 11B39, 11P05, 11A51

❖❖❖