ON FIBONACCI NUMBERS AND PRIMES OF THE FORM $4k + 1$

Neville Robbins
Mathemetics Department, San Francisco State University, San Francisco, CA 94132
(*Submitted February 1992*)

A well-known theorem of elementary number theory states:

$$\text{There exist infinitely many primes } p \text{ such that } p \equiv 1 \pmod 4. \tag{I}$$

(See [1], p. 224.)

One can prove (I) constructively by generating an infinite sequence $\{p_n\}$ of distinct primes such that $p_n \equiv 1 \pmod 4$ for all $n \geq 1$. To obtain the sequence $\{p_n\}$, let $\{u_n\}$ be a sequence of natural numbers such that:

(i) $u_n > 1$ for all $n \geq 1$.

(ii) If q is prime and $q | u_n$, then $q \equiv 1 \pmod 4$.

(iii) $(u_m, u_n) = 1$ for all $m \neq n$.

If we let p_n be the least prime divisor of u_n for all $n \geq 1$, then the sequence $\{p_n\}$ yields the desired result.

Let $u_n = a_n^2 + b_n^2$ where a_n, b_n are natural numbers such that $(a_n, b_n) = 1$ and $a_n \not\equiv b_n \pmod 2$. Then the sequence $\{u_n\}$ satisfies (i) and (ii). If (iii) also holds, then $\{u_n\}$ fulfills all our requirements.

Customarily, one lets $u_n = \phi_n = 2^{2^n} + 1$, the n^{th} Fermat number. If $n \geq 1$, then

$$\phi_n = (2^{2^{n-1}})^2 + 1^2,$$

where $2^{2^{n-1}}$ and 1 are relatively prime and of opposite parity. Since it is also true that $(\phi_m, \phi_n) = 1$ for all $m \neq n$, we are done.

An alternative procedure utilizes the Fibonacci sequence $\{F_n\}$ or, more precisely, an infinite subsequence thereof. We need the following properties of Fibonacci numbers:

$$F_{2k+1} = F_k^2 + F_{k+1}^2. \tag{1}$$

$$(F_m, F_n) = F_{(m,n)}. \tag{2}$$

$$2 | F_n \text{ iff } 3 | n. \tag{3}$$

$$\text{If } n \geq 3, \text{ then } F_n > 1. \tag{4}$$

(See [2].)

Suppose we number the primes starting with 5 as follows: $q_1 = 5, q_2 = 7, q_3 = 11$, etc. Let $u_n = F_{q_n}$ for $n \geq 1$. Now (1) implies

$$F_{q_n} = F^2_{\frac{1}{2}(q_n - 1)} + F^2_{\frac{1}{2}(q_n+1)} \text{ for all } n \geq 1.$$

Since $\left(\frac{1}{2}(q_n - 1), \frac{1}{2}(q_n + 1)\right) = 1$, (2) implies

$$\left(F_{\frac{1}{2}(q_n-1)}, F_{\frac{1}{2}(q_n+1)}\right) = F_1 = 1.$$

Since $q_n > 3$ and q_n is prime by definition, (3) implies $2 \nmid F_{q_n}$, so

$$F_{\frac{1}{2}(q_n-1)} \not\equiv F_{\frac{1}{2}(q_n+1)} \pmod 2.$$

Finally, if $m \neq n$, then $q_m \neq q_n$, so $(q_m, q_n) = 1$. Therefore, (2) implies $(F_{q_m}, F_{q_n}) = 1$.

In summary, an infinitude of primes p such that $p \equiv 1 \pmod 4$ can be obtained by considering the least prime divisors of the various Fibonacci numbers F_q, where q is prime and $q \geq 5$.

REFERENCES

1. David M. Burton. *Elementary Number Theory.* 2nd ed. New York: Wm. C. Brown, 1988.
2. Verner E. Hoggatt, Jr. *Fibonacci and Lucas Numbers.* Boston: Houghton-Mifflin, 1969; rpt. Santa Clara, CA: The Fibonacci Association 1980.

AMS Classification Number: 11B35

❖❖❖