GENERALIZATION OF A THEOREM OF DROBOT

Lawrence Somer
Dept. of Math., The Catholic University of America, Washington, DC 20064
e-mail: somer@cua.edu

(*Submitted September 2000-Final Revision December 2000*)

It is well known that the Fibonacci number F_n can be a prime only if $n = 4$ or $n = p$, where p is an odd prime. Throughout this paper, p will denote a prime. In a very interesting paper, Drobot [2] proved that F_p is composite for certain primes p. In particular, he proved that if $p > 7$, $p \equiv 2$ or 4 (mod 5), and $2p-1$ is also a prime, then $2p-1 \mid F_p$ and $F_p > 2p-$. For example, $37 \mid F_{19} = 4181 = 37 \cdot 113$.

A similar result was proved by Euler and, independently, by Lagrange about the Mersenne numbers. It is easy to see that the Mersenne number $M_n = 2^n - 1$ can be a prime only if n is a prime. Euler and Lagrange proved that, if $p \equiv 3 \pmod 4$ and $2p+1$ is also a prime, then $2p+1 \mid M_p = 2p+1$. A proof of this result is given in [5, pp. 90-91].

The primality of Mersenne numbers is of interest because of the following relationship to even perfect numbers. A positive integer is perfect if it is equal to the sum of its proper divisors. Euclid and Euler proved that the even integer n is perfect if and only if n is of the form $2^{p-1}(2^p - 1)$, where $2^p - 1$ is a Mersenne prime. Euclid proved that this condition is sufficient for n to be a perfect number and Euler proved the necessity of this condition. At the present time only thirty-eight Mersenne primes are known, with the largest known Mersenne prime being $2^{6972593} - 1$, which has over two million digits. A list of all known Mersenne primes is given in the web site

http://www.utm.edu/research/primes/glossary/Mersennes.html.

We will prove a theorem which generalizes both of the results given above concerning the compositeness of F_p and M_p. Before presenting this theorem, we will need the following definition and results involving Lucas sequences.

Definition 1: The Lucas sequence $u(a, b)$ is a second-order linear recurrence satisfying the relation $u_{n+2} = au_{n+1} + bu_n$ and having initial terms $u_0 = 0$, $u_1 = 1$, where a and b are integers.

We let $D = a^2 + 4b$ be the discriminant of $u(a, b)$. Associated with $u(a, b)$ is the characteristic polynomial $f(x) = x^2 - ax - b$ with characteristic roots α and β. Then, by the Binet formula

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}. \tag{1}$$

We have the following theorem concerning the divisibility of u_n by the prime p.

Theorem 1: Let $u(a, b)$ be a Lucas sequence. Let p be an odd prime such that $p \nmid bD$. Then

$$p \mid u_{p-(D/p)}, \tag{2}$$

where (D/p) is the Legendre symbol. Moreover,

$$p \mid u_{(p-(D/p))/2} \tag{3}$$

if and only if $(-b/p) = 1$.

Proof: Proofs of (2) are given in [4, pp. 290, 296-97] and [1, pp. 44-45]. A proof of (3) is given in [3, p. 441]. □

We are now ready for our main result, Theorem 2. The results by Drobot and by Euler and by Lagrange on the compositeness of F_p and M_p will then be given as corollaries of Theorem 2.

Theorem 2: Let $u(a, b)$ be a Lucas sequence. Let p be an odd prime such that $p \nmid b$.

(a) If $2p-1$ is a prime, $(D/(2p-1)) = -1$, and $(-b/(2p-1)) = 1$, then $2p-1 \mid u_p$.

(b) If $2p+1$ is a prime, $(D/(2p+1)) = 1$, and $(-b/(2p+1)) = 1$, then $2p+1 \mid u_p$.

Proof: ***(a)*** By (3), $2p-1 \mid u_{(2p-1+1)/2} = u_p$. ***(b)*** By (3), $2p+1 \mid u_{(2p+1-1)/2} = u_p$. □

Corollary 1 (Drobot): Let p be a prime such that $p > 7$, $p \equiv 2$ or 4 (mod 5), and $2p-1$ is a prime. Then $2p-1 \mid F_p$ and $F_p > 2p-1$.

Proof: Note that $\{F_n\} = u(1, 1)$ and $D = 5$. It is clear from (1) that if $p > 7$, then $F_p > 2p-1$. If $p \equiv 2 \pmod 5$, then $2p-1 \equiv 3 \pmod 5$, while if $p \equiv 4 \pmod 5$, then $2p-1 \equiv 2 \pmod 5$. By the law of quadratic reciprocity, if $2p-1 \equiv 2$ or 3 (mod 5), then

$$(D/(2p-1)) = (5/(2p-1)) = -1.$$

Since $p \equiv 1$ or 3 (mod 4), it follows that $2p-1 \equiv 1 \pmod 4$. Hence,

$$(-b/(2p-1)) = (-1/(2p-1)) = 1.$$

It now follows from Theorem 2(a) that

$$2p-1 \mid F_p. \quad \square$$

Corollary 2 (Euler and Lagrange): Let p be a prime such that $p > 3$, $p \equiv 3 \pmod 4$, and $2p+1$ is a prime. Then $2p+1 \mid M_p$ and $M_p > 2p+1$.

Proof: It is clear that if $p > 3$, then $M_p = 2^p - 1 > 2p+1$. Consider the Lucas sequence $u(3, -2)$. Then $D = 1$ and, by the Binet formula (1),

$$u_n = \frac{2^n - 1}{2-1} = 2^n - 1 = M_n.$$

Moreover,

$$(D/(2p+1)) = (1/(2p+1)) = 1.$$

It also follows from the fact that $p \equiv 3$ or 7 (mod 8) that $2p+1 \equiv 7 \pmod 8$. Thus,

$$(-b/(2p+1)) = (2/(2p+1)) = 1.$$

It now follows from Theorem 2(b) that

$$2p+1 \mid u_p = M_p. \quad \square$$

Remark: Primes p such that $2p+1$ is also a prime are called *Sophie Germain primes of the first kind*, while primes p such that $2p-1$ is a prime are called *Sophie Germain primes of the second kind*. It is not known whether there exist infinitely many Sophie Germain primes of the first or second kind. At the present time, the largest known Sophie Germain prime of the first kind is $3714089895285 \cdot 2^{60000} - 1$ with 18075 digits, and the largest known Sophie Germain prime of the

second kind is $16769025 \cdot 2^{34071} + 1$ with 10264 digits. For a list of the largest known Sophie Germain primes, see the web sites

http://www.utm.edu/research/primes/lists/top20/SophieGermain.html

and

http://ksc9.th.com/warut/cunningham.html.

ACKNOWLEDGMENT

I wish to thank the anonymous referee for his or her helpful suggestions which improved the presentation of this paper.

REFERENCES

1. R. D. Carmichael. "On the Numerical Factors of the Arithmetic Forms $\alpha^n \pm \beta^n$." *Ann. of Math.* **15** (1913):30-70.
2. V. Drobot. "On Primes in the Fibonacci Sequence." *The Fibonacci Quarterly* **38.1** (2000): 71-72.
3. D. H. Lehmer. "An Extended Theory of Lucas' Functions." *Ann. of Math.* **31** (1930):419-448.
4. E. Lucas. "Théorie des Fonctions Numériques Simplement Périodiques." *Amer. J. Math.* **1** (1878):184-240, 289-321.
5. P. Ribenboim. *The New Book of Prime Number Records*. New York: Springer-Verlag, 1996.

AMS Classification Numbers: 11A51, 11B39

❖❖❖