ANOTHER PROOF THAT $\phi(F_n) \equiv 0$ MOD 4 FOR ALL $n > 4$

VERNER E. HOGGATT, JR., and HUGH EDGAR
San Jose State University, San Jose, CA 95192

1. INTRODUCTION AND DISCUSSION

The problem, as originally proposed by Douglas Lind [1], was as follows:

If F_n is the nth Fibonacci number, then show that

$$\phi(F_n) \equiv 0 \pmod 4,\ n > 4, \text{ where } \phi(n) \text{ is Euler's } \phi\text{-function.}$$

An incomplete solution due to John L. Brown, Jr., appeared in [2]. The problem resurfaced in Problem E 2581, proposed by Clark Kimberling [3]. An extremely elegant solution was given by Peter Montgomery [4].

The main object of this note is to provide another solution to the original problem cited and some generalizations [5]. However, before giving our solution, we cannot resist redocumenting Montgomery's simple and beautiful solution:

Consider the set $H = \{-F_{n-1}, -1, +1, F_{n-1}\}$. The first observation is that the elements of this set are pairwise incongruent modulo F_n. Only four of the $\binom{4}{2}$ incongruences to be checked are distinct, and three of these four are trivialities. The most interesting of these is $F_{n-1} \not\equiv -F_{n-1} \pmod{F_n}$, which can easily be done by showing that $F_n < 2F_{n-1} < 2F_n$ so that $F_n \mid 2F_{n-1}$ is impossible. Second, since $(F_n, F_{n-1}) = 1$, the set H is a subset of $(Z/F_nZ)^*$, the multiplicative group (under multiplication modulo F_n) of units of the ring Z/F_nZ (see S. Lang [6]). Finally, since $F_{n-1}^2 - F_{n-2}F_n = (-1)^n$, it follows that H is closed under multiplication and hence (being finite) is a subgroup of $(Z/F_nZ)^*$. However, the order of $(Z/F_nZ)^*$ is $\phi(F_n)$, and the order of subgroup H is 4, so that the conclusion follows from Lagrange's Theorem: "The order of a subgroup of a finite group divides the order of the group." The basic ideas of Montgomery's proof have been extended to generalized Fibonacci numbers satisfying $u_{n+1}u_{n-1} - u_n^2 = \pm 1$ in [5].

2. ANOTHER PROOF

Our proof breaks up into two parts. The first part characterizes those positive integers m for which $4 \nmid \phi(m)$. The second part shows that $F_n \neq m$, whenever $n > 4$. $\phi(1) = \phi(2) = 1$, and $2 \mid \phi(m)$ for all positive integers $m \geq 3$, so that the first part of our proof amounts to characterizing those positive integers m for which $2 \parallel \phi(m)$ [i.e., $2 \mid \phi(m)$ but $2^2 \nmid \phi(m)$]. If the canonical decomposition of m is

$$m = p_1^{e_1} p_2^{e_2} \ldots p_g^{e_g},$$

then

$$\phi(m) = p_1^{e_1-1} p_2^{e_2-1} \ldots p_g^{e_g-1}(p_1 - 1)(p_2 - 1) \ldots (p_g - 1),$$

where $2 \leq p_1 < p_2 < \ldots < p_g$ and $p_1, p_2, \ldots, p_g$ are primes.

If $p_1 = 2$, then $m = 2^{e_1} p_2^{e_2} \ldots p_g^{e_g}$, and

$$\phi(m) = 2^{e_1-1} p_2^{e_2-1} p_3^{e_3-1} \ldots p_g^{e_g-1}(2 - 1)(p_2 - 1)(p_3 - 1) \ldots (p_g - 1).$$

This requirement forces $1 \leq e_1 < 2$. If $e_1 = 2$, then $g = 1$ is forced and m must be 4. If $e_1 = 1$, then

$$\phi(m) = p_2^{e_2-1}p_3^{e_3-1} \ldots p_g^{e_g-1}(p_2 - 1)(p_3 - 1) \ldots (p_g - 1)$$

so that $g = 2$ is forced, and $m = 2p^e$ for some odd prime p and some positive integer e. Furthermore, $p \equiv 3 \pmod 4$ must obtain. If $p_1 > 2$, we must have $g = 1$ so that $m = p^e$, where the conditions on p and e are precisely as above. Summarizing, we have shown that $4 \nmid \phi(m)$ if and only if $m = 1, 2, 4p^e$, or $2p^e$, where p is any prime satisfying $p \equiv 3 \pmod 4$ and e is any positive integer.

If now suffices to prove that $F_n \neq 1, 2, 4p^e$, or $2p^e$ whenever $n > 4$, where p is a prime such that $p \equiv 3 \pmod 4$ and e is a positive integer.

Case 1: $F_n = p \equiv 3 \pmod 4$, p a prime, is impossible if $n > 4$.

If n is even, then $n \geq 6$ and $F_n = F_{2k} = F_k L_k$, where $k \geq 3$. Since $F_k > 1$ and $L_k > 1$ whenever $k \geq 3$, it follows that F_n is composite.

If n is odd, then $F_n = F_{2k+1} = F_k^2 + F_{k+1}^2 \not\equiv 3 \pmod 4$.

Case 2: $F_n = 2p$ with $p \equiv 3 \pmod 4$ and p a prime is impossible.

If $n > 4$, $F_6 = 8$ is not of the prescribed form. If n is even and $n \geq 8$, then $F_n = F_{2k}L_k = 2p$ is impossible since $k \geq 4$ forces $F_k > 2$ and $L_k > 2$. If n is odd, then $F_n = 2p = F_{2k+1} = F_{6r+3}$ because $2|F_n$ if and only if $3|n$. Hence, $F_{2r+1}|F_{6r+3} = 2p$ since $2r + 1|6r + 3$. $F_9 = 34 = 2 \cdot 17$, but $17 \not\equiv 3 \pmod 4$. Otherwise, $2 < F_{2r+1} < F_{6r+3}$ and $F_{2r+1} \neq p$ by Case 1, and so Case 2 is complete.

Case 3: $F_n = p^e$ with $p \equiv 3 \pmod 4$ and p a prime is impossible.

If $n > 4$, then we may assume that the positive integer e is greater than one, because of Case 1. If n is even, then $F_n = F_{2k} = F_k L_k$ with $(F_k, L_k) = 1$ or 2, a contradiction. If n is odd, then $F_n = F_{2k+1}$ and $2k + 1 \equiv 3 \pmod 6$, since we cannot tolerate $2|F_n$. Hence, $2k + 1 \equiv \pm 1 \pmod 6$ must obtain, which forces $F_n \equiv 1 \pmod 4$, and so $2|e$. However, the only Fibonacci squares are $F_1 = F_2 = 1$ and $F_{12} = 144$, and so Case 3 is complete.

Case 4: $F_n = 2p^e$ with $p \equiv 3 \pmod 4$, p a prime, is impossible.

By Case 2, we can assume $e > 1$. Since $2|F_n$, we must have $3|n$, and so $F_n = F_{3k} = 2p^e$. If $2|k$, then $6|n$, and hence $8 = F_6|F_n$, a contradiction, so $k = 2r + 1$, and $F_{2r+1}|F_{6r+3} = F_{3k} = F_n = 2p^e \equiv 2 \pmod 4$. $F_{2r+1} \neq 2$, once $r > 1$. $F_{2r+1} \neq p$, by Case 1; $F_{2r+1} \neq 2p$, by Case 2; and $F_{2r+1} \neq p^t$ for any integer t such that $0 \leq t \leq e$, by Case 3; so $F_{2r+1} = 2p^s$ is forced for some positive integer $s < r$. Let r be the least subscript for which F_{2r+1} is of this form. Since $2|F_{2r+1}$, $F_{2r+1} = F_{6n+3}$ for some suitable positive integer n. Thus, $F_{2r+1} = F_{6n+3} = 2p^s$, and $F_{2n+1}|F_{6n+3} = 2p^s$. But now $F_{2n+1} = 2p^t$ for suitable positive integral t is forced, contradicting the minimal nature of subscript r. The proof of Case 4, and with it the solution to the original problem, is complete.

REFERENCES

1. Douglas Lind. Problem H-54. *The Fibonacci Quarterly* 3, No. 1 (1965): 44.
2. John L. Brown, Jr. (Incomplete Solution to H-54). *The Fibonacci Quarterly* 4, No. 4 (1966):334-335.
3. Clark Kimberling. Problem E 2581. *American Math. Monthly*, March 1976, p. 197.
4. Peter Montgomery. Solution to E 2581. *American Math. Monthly*, June-July 1977, p. 488.

5. Verner E. Hoggatt, Jr., & Marjorie Bicknell-Johnson. "Generalized Fibonacci Numbers Satisfying $u_{n+1}u_{n-1} - u_n^2 = \pm 1$." *The Fibonacci Quarterly* 16, No. 2 (1978):130-137.
6. Serge Lang. *Algebraic Number Theory.* Reading, Mass.: Addison-Wesley Publishing Company, 1970. P. 65.

*****

LETTER TO THE EDITOR

DAVID L. RUSSELL
University of Southern California, University Park, Los Angeles, CA 90007

Dear Professor Hoggatt:

. . . In response to your request for me to point out the errors in your article "A Note on the Summation of Squares," *The Fibonacci Quarterly* 15, No. 4 (1977):367-369, . . . I have enclosed a xerox copy of your paper with corrections marked. The substantive errors occur in the top two equations of p. 369, where an incorrect sign and some minor errors result in an incorrect denominator for the RHS. As an example, consider the case $p = 1$, $q = 2$, $n = 4$; your formula evaluates to 0, which is clearly incorrect:

$$P_0 = 0,\ P_1 = 1,\ P_2 = 1,\ P_3 = 3,\ P_4 = 5,\ P_5 = 11,\ P_6 = 21;$$
$$8P_5P_4 - (P_6^2 - 1) = (8)(11)(5) - 440 = 0.$$

Only if the denominator is also zero does a numerator of zero make sense.

Sincerely yours,
[*David L. Russell*]

CORRECTIONS TO "A NOTE ON THE SUMMATION OF SQUARES" BY VERNER E. HOGGATT, JR.

The following corrections to the above article were noted by Prof. David L. Russell.

Page 368: The equation on line 19, $q^{n-1}P_2P_1 = q^{n-1}P_1^2 + q^nP_1P_0$, should be:

$$q^nP_2P_1 = q^nP_1^2 + q^{n+1}P_1P_0$$

The equation on line 27, $P_{j+2}^2 = P^2P_{j+1}^2 + q^2P_j^2 + 2pqP_jP_{j+1}$, should be:

$$P_{j+2}^2 = p^2P_{j+1}^2 + q^2P_j^2 + 2pqP_jP_{j+1}$$

In the partial equation on line 32 (last line) the = sign should be a - (minus) sign.

Page 369: Lines 1-11 should read:

$$pP_{n+1}^2 + \left(\sum_{j=1}^{n} P_j^2\right)\left(p + \frac{(1-q)(p^2+q^2-1)}{2pq}\right)$$
$$= P_{n+2}P_{n+1} + \frac{1-q}{2pq}[P_{n+2}^2 + P_{n+1}^2 - 1 - p^2P_{n+1}^2]$$