Canad. Math. Bull. Vol. **25** (3), 1982

A NOTE ON THE FIBONACCI QUOTIENT $F_{p-\varepsilon}/p$.

BY
H. C. WILLIAMS

ABSTRACT. In this note a formula analogous to Eisenstein's well known formula is presented for $F_{p-\varepsilon}/p$, where F_n is the nth Fibonacci number ($F_0=0, F_1=1$), p an odd prime, and

$$\varepsilon=\begin{cases}1 & p\equiv\pm1 \pmod 5\\ -1 & p\equiv\pm2 \pmod 5).\end{cases}$$

This formula is:

$$F_{p-\varepsilon}/p\equiv\frac{2}{5}\sum_{k=1}^{p-1-[p/5]}\left(\frac{-1}{k}\right)^k \pmod p \quad (p\neq 5).$$

1. **Introduction.** Let F_n be the nth Fibonacci number, where $F_0=0$, $F_1=1$, and $F_{k+1}=F_k+F_{k-1}$. It is well known that if p ($\neq 5$) is a prime, then

$$p \mid F_{p-\varepsilon}, \quad \text{where} \quad \varepsilon=\begin{cases}1 & \text{when} \quad p\equiv\pm1 \pmod 5\\ -1 & \text{when} \quad p\equiv\pm2 \pmod 5\end{cases}$$

That is, $\varepsilon=(5\mid p)$, where $(a\mid p)$ is the Legendre Symbol. In 1960 Wall [5] posed the problem of whether there exists a prime p such that $p^2\mid F_{p-\varepsilon}$. It is still not known whether such a prime exists although it is known (Williams, unpublished) that it must exceed 10^9. This problem is analogous to the famous problem concerning the existence of primes p such that

$$2^{p-1}\equiv 1 \pmod{p^2}.$$

Here, however, two solutions 1093 and 3511 are known. There are no other solutions for $p<5.4\times10^9$ (Brillhart *et al.* [2]; Lehmer, unpublished).

One rather pretty result concerning the Fermat quotient $(2^{p-1}-1)/p$ is that of Eisenstein (cf. Dickson [3, p. 105]).

$$(1.1) \qquad (2^{p-1}-1)/p\equiv-\frac{1}{2}\sum_{k=1}^{p-1}\left(\frac{-1}{k}\right)^k \pmod p \qquad (p\neq 2).$$

In [1] Andrews found formulae which are analogous to (1.1) for $F_{p-\varepsilon}/p$. These results were given as

$$F_{p-1}/p\equiv 2(-1)^{(p-1)/2}\sum_{\substack{m\equiv 7,5 \pmod{10}\\ |m|<p}}\frac{(m+1\mid 5)(-1\mid m)}{p-m} \pmod p$$

Received by the editors April 25, 1980.
AMS (1980) Classification numbers: 10A35, 10A10.
Key Words and phrases: Fibonacci numbers.

for $p \equiv \pm 1 \pmod 5$ and

$$F_{p+1}/p \equiv 2(-1)^{(p-1)/2} \sum_{\substack{m \equiv 1,5 \pmod{10} \\ |m|<p}} \frac{(m+1 \mid 5)(-1 \mid m)}{p-m} \pmod p$$

for $p \equiv \pm 2 \pmod 5$. Unfortunately, these rather complicated formulae are not as attractive as the simple formula of (1.1). In this note we present a much simpler formula than those given above for $F_{p-\varepsilon}$. Our method of proof is elementary and quite different from that of [1].

2. **Preliminary results.** Let α, β be the zeros of x^2-x-1 and let $\{L_n\}$ be the Lucas sequence defined by $L_0=2$, $L_1=1$, $L_{k+1}=L_k+L_{k-1}$. From the Binet formulae,

$$L_n = \alpha^n + \beta^n \tag{2.1}$$

$$F_n = (\alpha^n - \beta^n)/(\alpha - \beta), \tag{2.2}$$

it is easy to derive the well-known results

$$2L_{n+m} = L_nL_m + 5F_nF_m, \tag{2.3}$$

$$2F_{n+m} = L_nF_m + F_nL_m, \tag{2.4}$$

$$L_{-n} = (-1)^nL_n, \qquad F_{-n} = (-1)^{n+1}F_n, \tag{2.5}$$

$$L_n^2 - 5F_n^2 = 4(-1)^n. \tag{2.6}$$

In the work that follows we assume that p is an arbitrary but fixed prime which is neither 2 nor 5. From (2.3), (2.4), and (2.5), we see that

$$2L_{p-\varepsilon} = 5F_p - \varepsilon L_p, \tag{2.7}$$

$$2F_p = F_{p-\varepsilon} + \varepsilon L_{p-\varepsilon}. \tag{2.8}$$

On putting $n = p - \varepsilon$ in (2.6) and using the fact that $p \mid F_{p-\varepsilon}$, we get $L^2_{p-\varepsilon} \equiv 4 \pmod{p^2}$ or

$$(L_{p-\varepsilon} - 2)(L_{p-\varepsilon} + 2) \equiv 0 \pmod{p^2}.$$

Since $L_{p-\varepsilon} \equiv 2\varepsilon \pmod p$ (see for example, Lehmer [4, p. 423]) and $p \nmid (L_{p-\varepsilon} - 2, L_{p-\varepsilon} + 2)$, we see that

$$L_{p-\varepsilon} \equiv 2\varepsilon \pmod{p^2}. \tag{2.9}$$

It follows from (2.9) and (2.8) that

$$F_{p-\varepsilon} \equiv 2\varepsilon(F_p - \varepsilon) \pmod{p^2}. \tag{2.10}$$

3. **The main result.** Since $\alpha + \beta = 1$ and $\alpha\beta = -1$, we can put

$$\alpha = -\omega - \omega^4, \qquad \beta = -\omega^3 - \omega^2, \tag{3.1}$$

where ω is a primitive 5th root of unity; that is,

$$\omega^4+\omega^3+\omega^2+\omega+1=0. \tag{3.2}$$

Put

$$T_i=\sum_{k=0}^{[p/5]}\binom{p}{5k+i} \qquad (i=0,1,2,3,4),$$

where $[p/5]$ is the largest integer less than $p/5$. We note that

$$\sum_{i=0}^{4} T_i=2^p. \tag{3.3}$$

We are now able to prove

THEOREM 1. *With the symbols defined above we have*

$$5F_p\equiv\varepsilon(5T_0-2^p-2) \pmod{p^2}.$$

Proof. From (2.1), (2.2), and (3.1), we get

$$\begin{aligned}(-\omega^3-\omega^2+\omega+\omega^4)F_p&=(\omega+\omega^4)^p-(\omega^3+\omega^2)^p\\&=\omega^{4p}\sum_{i=0}^{p}\binom{p}{i}\omega^{2i}-\omega^{2p}\sum_{i=0}^{p}\binom{p}{i}\omega^{i}\\&=\omega^{-p}(T_0+\omega^2T_1+\omega^4T_2+\omega T_3+\omega^3T_4\\&\quad-\omega^{2p}(T_0+\omega T_1+\omega^2T_2+\omega^3T_3+\omega^4T_4)\end{aligned}$$

and

$$\begin{aligned}-L_p&=\omega^{-p}(T_0+\omega^2T_1+\omega^4T_2+\omega T_3+\omega^3T_4)\\&\quad+\omega^{2p}(T_0+\omega T_1+\omega^2T_2+\omega^3T_3+\omega^4T_4).\end{aligned}$$

If $p\equiv 1 \pmod 5$, we get

$$-L_p=2T_3+\omega^2(T_0+T_4)+\omega(T_1+T_4)+\omega^4(T_0+T_2)+\omega^3(T_2+T_1) \tag{3.4}$$

and

$$(-\omega^3-\omega^2+\omega+\omega^4)F_p=\omega^2(T_4-T_0)+\omega(T_1-T_4)+\omega^4(T_0-T_2)+\omega^3(T_2-T_1).$$

Thus,

$$\omega^2(T_4-T_0+F_p)+\omega(T_1-T_4-F_p)+\omega^4(T_0-T_2-F_p)+\omega^3(T_2-T_1+F_p)=0.$$

Since (3.2) is irreducible, we can only have

$$F_p=T_0-T_4=T_1-T_4=T_0-T_2=T_1-T_2 \tag{3.5}$$

and

$$T_2=T_4, \qquad T_0=T_1. \tag{3.6}$$

https://doi.org/10.4153/CMB-1982-053-0 Published online by Cambridge University Press

Hence, from (3.3) and (3.6), we get

$$T_3+2T_0+2T_2=2^p \tag{3.7}$$

and from (3.4), (3.6), and (3.7), we have

$$L_p=5(T_0+T_2)-2^{p+1}. \tag{3.8}$$

Since $\varepsilon=1$, we find from (2.7), (2.9), (3.5), and (3.8) that

$$5T_2\equiv 2^p-2 \pmod{p^2}. \tag{3.9}$$

The result of the theorem now follows from (3.5) and (3.9).

It can be shown in a similar manner that this same result is true for $p\equiv 2$, 3, 4 (mod 5). □

We are now able to give our main result as

THEOREM 2. *If p is any prime except* 2 *or* 5, *then*

$$F_{p-\varepsilon}/p\equiv\frac{2}{5}\sum_{k=1}^{p-1-[p/5]}\frac{(-1)^k}{k} \pmod{p}. \tag{3.10}$$

Proof. From (2.10) and the result of Theorem 1, we have

$$F_{p-\varepsilon}\equiv\tfrac{2}{5}(5(T_0-1)-2^p-2) \pmod{p^2}. \tag{3.11}$$

Since

$$\binom{p}{i}\equiv\frac{p}{i}(-1)^{i+1} \pmod{p^2} \qquad (0<i<p)$$

and

$$T_0-1=\sum_{k=1}^{[p/5]}\binom{p}{5k},$$

we see that

$$5(T_0-1)\equiv p\sum_{k=1}^{[p/5]}\frac{(-1)^{k+1}}{k} \pmod{p^2}$$

Using this result together with (1.1) and (3.11), we get

$$F_{p-\varepsilon}/p\equiv\frac{2}{5}\left(\sum_{k=1}^{p-1}\frac{(-1)^k}{k}-\sum_{k=1}^{[p/5]}\frac{(-1)^k}{k}\right)$$

$$\equiv\frac{2}{5}\sum_{k=1}^{p-1-[p/5]}\frac{(-1)^k}{k} \pmod{p}. \quad \square$$

This result (3.10) is much simpler than the results given by Andrews and seems to be more strictly analogous to (1.1). Unfortunately, the method of proof here made use of very special properties of the Fibonacci sequence. It is not known whether simple results, results similar to (1.1) or (3.10) exist for other Lucas sequences such as the Pell sequence.

References

1. G. H. Andrews, *Some Formulae for the Fibonacci sequence with generalizations*, Fib. Quart., **7** (1969), 113–130.

2. J. Brillhart, J. Tonascia, and P. Weinberger, *On the Fermat quotient, Computers in Number Theory*, Academic Press, London and New York, 1971, pp 213–222.

3. L. E. Dickson, *History of the Theory of Numbers*, Vol. 1, Chelsea, New York, 1952.

4. D. H. Lehmer, *An extended theory of Lucas' functions*, Annals of Math. (2) **31** (1930), 419–448.

5. D. D. Wall, *Fibonacci series modulo m*, Amer. Math. Monthly, **67** (1960), 525–532.

Department of Computer Science
University of Manitoba
Winnipeg, Manitoba, R3T 2N2
Canada.