ON A CONGRUENCIAL PROPERTY OF FIBONACCI NUMBERS

— CONSIDERATIONS AND REMARKS —

MASATAKA YORINAGA

In a previous note with the same title [4], we have examined on a computer the possibility of the converse of the following proposition, obtaining several counter examples to it :

Proposition. *If N is a prime number $\neq 5$, then we have*

$$U_N \equiv \left(\frac{N}{5}\right) \pmod{N},$$

where U_N denotes the N-th Fibonacci number and $(N/5)$ is the Legendre symbol.

In the present note, we shall try to weaken the restriction for N to be a prime, thus extending this proposition. We have found, as a result, that this can actually be achieved to some extent (cf. our Theorem below).

We define the numbers V_n $(n=1, 2, \cdots)$ by setting

$$V_n = \frac{U_{2n}}{U_n}.$$

The sequence (V_n) is known as the so-called associated Lucas sequence [1, 2]. The numbers U_n and V_n can be written in the form, with $a=(1+\sqrt{5})/2$, $b=(1-\sqrt{5})/2$,

$$(1) \qquad U_n = \frac{a^n - b^n}{\sqrt{5}}, \quad V_n = a^n + b^n \quad (n = 1, 2, \cdots).$$

If an integer $N > 0$, $\neq 5$, satisfies the relation

$$U_N \equiv \left(\frac{N}{5}\right) \pmod{N},$$

we shall call N a converse number. When a prime number p retains the property that some U_n with $n>1$ is divisible by p, but for any integer m, $0<m<n$, U_m is not divisible by p, we call p a primitive (prime) factor of U_n. It is known that every Fibonacci number U_n with n $\neq 1$, 2, 6 or 12 admits a primitive factor (cf. [3 ; §2]). A prime factor

q of U_n which is not primitive will be called an elementary factor of U_n.

The proper part of U_n is the number which is obtained by removing all the elementary factors from U_n. In the subsequent discussions, we always assume that $n>5$ in U_n, so that the proper part of any U_n under consideration is an odd integer which does not contain the number 5 as a factor.

Lemma 1. *If p is a primitive factor of a number U_n, then p can be written in the linear form:*

$$p = nk + 1 \qquad \textit{if} \ \left(\frac{p}{5}\right) = 1,$$

$$p = nk - 1 \qquad \textit{if} \ \left(\frac{p}{5}\right) = -1$$

with some positive integer k.

This lemma is an immediate consequence of the proposition quoted in the previous note [4] and is a well-known result.

Lemma 2. *If N is a divisor of the proper part of some U_n, then N can be written in the form:*

$$N = nk + 1 \qquad \textit{if} \ \left(\frac{N}{5}\right) = 1,$$

$$N = nk - 1 \qquad \textit{if} \ \left(\frac{N}{5}\right) = -1$$

with some positive integer k.

Proof. We shall prove the lemma in the case where N is the product of two primitive factors p_1 and p_2 of U_n; the general case can be treated in quite a similar way. Put $s_1=(x_1/5)$, $s_2=(p_2/5)$ and $s=(N/5)=s_1s_2$. Since, by virtue of Lemma 1, $p_1=nk_1+s_1$ and $p_2=nk_2+s_2$ for some k_1, $k_2>0$, we have then

$$(2) \qquad N = p_1p_2 = n(nk_1k_2 + s_2k_1 + s_1k_2) + s_1s_2.$$

From this expression, the assertion is obvious.

Lemma 3. *For any odd integer $N>0$, there hold the following relations:*

$$(3) \qquad U_N - (-1)^{(N-1)/2} = U_{(N-1)/2}V_{(N+1)/2},$$

$$(4) \qquad U_N - (-1)^{(N+1)/2} = U_{(N+1)/2}V_{(N-1)/2}.$$

Proof. By the expressions in (1), we have for any integer $n > 0$

$$U_n V_{n+1} = \frac{a^n - b^n}{\sqrt{5}} (a^{n+1} + b^{n+1})$$
$$= \frac{a^{2n+1} - b^{2n+1}}{\sqrt{5}} - (ab)^n \frac{a-b}{\sqrt{5}}$$
$$= U_{2n+1} - (-1)^n,$$

giving the first relation in the lemma. The proof for the second relation is quite the same.

Lemma 4. *If k is an odd integer > 0, then V_{kn} is divisible by V_n.*

Proof. By the second expression in (1) we have $V_n = a^n + b^n$ and $V_{kn} = a^{kn} + b^{kn}$, so that

$$\frac{V_{kn}}{V_n} = a^{(k-1)n} + b^{(k-1)n} - (ab)^n (a^{(k-3)n} + b^{(k-3)n}) + \cdots$$
$$+ (-1)^{(k-1)/2} (ab)^{(k-1)n/2},$$

whence the result.

In the subsequent lemmas, N denotes a divisor of the proper part of some U_n, $n > 5$, and we put $s = (N/5)$.

Lemma 5. *$U_{(N-s)/2}$ is divisible by N if $(N-s)/n$ is even, and $V_{(N-s)/2}$ is divisible by N if $(N-s)/n$ is odd.*

Proof. Note that $(N-s)/n$ is integral, by Lemma 2. We examine four cases according to the the sign of s and the parity of $k = (N-s)/n$.

1) The case of $s = 1$ and k even. In this case, $(N-1)/2$ is divisible by n. Therefore, $U_{(N-1)/2}$ is divisible by U_n. Consequently, $U_{(N-1)/2}$ is divisibleby N.

2) The case of $s = 1$ and k odd. This case is possible only when n is even, and $(N-1)/2$ is an odd multiple of $n/2$. Therefore, $V_{(N-1)/2}$ is divisible by $V_{n/2}$, by Lemma 4. Besides, when n is even, all primitive factors of U_n are always factors of $V_{n/2}$. Hence, $V_{(N-1)/2}$ is divisible by N.

3) The case of $s = -1$ and k even. In this case, $(N+1)/2$ is divisible by n. Therefore, $U_{(N+1)/2}$ is divisible by U_n. Hence, $U_{(N+1)/2}$ is divisible by N.

4) The case of $s = -1$ and k odd. This case is possible only when n is even. Then, as in the case 2), $V_{(N+1)/2}$ is divisible by $V_{n/2}$, and hence $V_{(N+1)/2}$ is divisible by N.

Lemma 6. *If n is odd, then N has the linear form:*

$$N = 4nk + 1 \qquad \text{if} \quad s = 1,$$
$$N = 4nk + 2n - 1 \qquad \text{if} \quad s = -1.$$

Hence, $(N - s)/n$ is always even.

Proof. We have $U_{2m+1} = U_m^2 + U_{m+1}^2$ for any integer $m > 0$. Therefore, N is a divisor of an integer of the form $x^2 + y^2$, where $(x, y) = 1$. Hence, in view of the property of quadratic residues, we must have $N \equiv 1 \pmod 4$. From this fact the lemma will follow easily.

Lemma 7. *When $n \equiv 0 \pmod 4$, then $(N - 1)/n$ is even if $s = 1$, and $(N + 1)/2$ is odd if $s = -1$.*

When $n \equiv 2 \pmod 4$, then we always have $s = 1$, and $(N - 1)/n$ may either be even or be odd.

Proof. Firstly, we examine the case where N consists only of one primitive factor p of U_n. And we classify the case into three.

1) The case of $n \equiv 0 \pmod 4$ and $s = 1$. Assume that $(p - 1)/n$ is odd. By the assumption and by Lemma 5, $V_{(p-1)/2}$ is divisible by p and $(p - 1)/2$ is even. We have, by (4),

$$U_p - (-1)^{(p+1)/2} = U_{(p+1)/2} V_{(p-1)/2},$$

where $U_p \equiv 1 \pmod p$ since p is a prime. Therefore, in the above expression,

the left-hand side $\equiv 2 \pmod p$, and
the right-hand side $\equiv 0 \pmod p$.

This is impossible. Hence, $(p - 1)/n$ must be even.

2) The case of $n \equiv 0 \pmod 4$ and $s = -1$. Assume that $(p + 1)/n$ is even. Then $U_{(p-1)/2}$ is divisible by p and $(p + 1)/2$ is even. From (4) we see that

$$U_p - (-1)^{(p+1)/2} = U_{(p+1)/2} V_{(p-1)/2},$$

where

the left-hand side $\equiv -2 \pmod p$, and
the right-hand side $\equiv 0 \pmod p$.

The contradiction assures that $(p+1)/n$ is odd.

3) The case of $n \equiv 2 \pmod 4$. Assume that $s = -1$. If we suppose in addition that $(p + 1)/n$ is even, then, in like manner as in the case 2), we arrive at a contradiction. In the sequel, we shall suppose that $(p + 1)/n$ is odd. Then, $(p + 1)/2$ is odd and $V_{(p+1)/2}$ is divisible by p.

From (3)

$$U_p - (-1)^{(p-1)/2} = U_{(p-1)/2} V_{(p+1)/2} ;$$

here

the left-hand side $\equiv -2 \pmod{p}$, and
the right-hand side $\equiv 0 \pmod{p}$.

Hence, it must be that $s=1$. About the fact that $(N-1)/n$ may be even or odd, we can readily confirm it by examples.

Now, for the proof of the general case it will suffice only to consider the case where N consists of two primitive factors p_1 and p_2 of U_n. Put $s_1=(p_1/5)$, $s_2=(p_2/5)$ and $p_1=nk_1+s_1$, $p_2=nk_2+s_2$.

4) The case of $n \equiv 0 \pmod 4$. By the expression (2), we have

$$\frac{N-s}{n} = nk_1k_2 + s_2k_1 + s_1k_2 .$$

Since the first term nk_1k_2 is even, as can be verified by arguing like above, the following scheme of implications clarifies all of the case :

$s=1$:
$s_1=s_2=1 \Longrightarrow k_1,\ k_2$ even $\Longrightarrow k_1+k_2$ even ;
$s_1=s_2=-1 \Longrightarrow k_1,\ k_2$ odd $\Longrightarrow k_1+k_2$ even ;
$s=-1$:
$s_1=1,\ s_2=-1 \Longrightarrow k_1$ even, k_2 odd $\Longrightarrow k_1-k_2$ odd ;
$s_1=-1,\ s_2=1 \Longrightarrow k_1$ odd, k_2 even $\Longrightarrow -k_1+k_2$ odd.

5) The case of $n \equiv 2 \pmod 4$.

From 3) we see that it is always true that $s_1=s_2=1$, and we obtain $s=s_1s_2=1$.

Now, our main result can be formulated in the following

Theorem. *If N is a divisor of the proper part of a Fibonacci number U_n with $n>5$, then N is a converse number.*

Proof. We divide the proof into five cases according to the sign of $s=(N/5)$ and the parity of n.

1) The case of n odd and $s=1$. In this case, by Lemma 6, $(N-s)/n$ is always even and, by Lemma 5, $U_{(N-1)/2}$ is divisible by N. In addition, we have $N=4nk+1$ by Lemma 6, so that $(N-1)/2$ is even. From the formula (3) we see

$$U_N - (-1)^{(N-1)/2} = U_{(N-1)/2} V_{(N+1)/2} \equiv 0 \pmod{N}.$$

Hence, we have $U_N \equiv 1 \pmod{N}$.

2) The case of n odd and $s=-1$. In this case, N has the linear form $N=4nk+2n-1$ by Lemma 6, so that $(N+1)/n$ is even. And,

$U_{(N-1)/2}$ is divisible by N and $(N+1)/2$ is odd. We have by (4)

$$U_N-(-1)^{(N+1)/2}=U_{(N+1)/2}V_{(N-1)/2}\equiv 0 \pmod{N}.$$

Hence, $U_N\equiv -1 \pmod{N}$.

3) The case of $n\equiv 0 \pmod 4$ and $s=1$. In this case, $(N-1)/n$ is even by Lemma 7. Therefore, $U_{(N+1)/2}$ is divisible by N and $(N-1)/2$ is even. We have by (3)

$$U_N-(-1)^{(N-1)/2}=U_{(N-1)/2}V_{(N+1)/2}\equiv 0 \pmod{N}.$$

Hence, $U_N\equiv 1 \pmod{N}$.

4) The case of $n\equiv 0 \pmod 4$ and $s=-1$. In this case, $(N+1)/n$ is odd by Lemma 7. Therefore, $V_{(N+1)/2}$ is divisible by N and $(N+1)/2$ is even. By (3)

$$U_N-(-1)^{(N-1)/2}=U_{(N-1)/2}V_{(N+1)/2}\equiv 0 \pmod{N}.$$

Hence, $U_N\equiv -1 \pmod{N}$.

5) The case of $n\equiv 2 \pmod 4$. In this case, we always have $s=1$. If $(N-1)/n$ is even, then $U_{(N-1)/2}$ is divisible by N and $(N-1)/2$ is even. By (3)

$$U_N-(-1)^{(N-1)/2}=U_{(N-1)/2}V_{(N+1)/2}\equiv 0 \pmod{N}.$$

Hence, $U_N\equiv 1 \pmod{N}$.

On the other hand, if $(N-1)/n$ is odd, then $V_{(N-1)/2}$ is divisible by N and $(N-1)/2$ is odd. We have by (4)

$$U_N-(-1)^{(N+1)/2}=U_{(N+1)/2}V_{(N-1)/2}\equiv 0 \pmod{N}.$$

Hence, $U_N\equiv 1 \pmod{N}$.

The proof of our theorem is now complete.

Numerical example 1. $N=4181=37\cdot 113$ is the proper part of U_{19}. Hence, N is a composite converse number. This example, which gives the least composite converse number, is one of the examples we have listed in the previous report [4].

Numerical example 2. $N=192900153617=2269\cdot 4373\cdot 19441$ is the proper part of U_{81}. Hence, $N_1=2269\cdot 4373$, $N_2=2269\cdot 19441$ and $N_3=4373\cdot 19441$, together with N, are all composite converse numbers.

Remark. The contraposition of the classical proposition cited in the first paragraph of this note gives rise to the following

Criterion. *If an integer* $N\not\equiv 0 \pmod 5$ *satisfies the relation*

$$U_N \not\equiv \left(\frac{N}{5}\right) \pmod{N},$$

then N *is a composite number.*

This criterion seems to be effective for the problem of factoring a large integer. However, our theorem shows that the above criterion does not provide any information, in the case of factorization of Fibonacci numbers at least.

REFERENCES

[1] L. E. DICKSON: History of the Theory of Numbers, Vol. I, Chelsea Publ. Co., New York, 1952.

[2] G. H. HARDY and E. M. WRIGHT: An Introduction to the Theory of Numbers, 3rd ed., Clarendon Press, Oxford, 1954.

[3] N. N. VOROB'EV: Fibonacci Numbers (English translation), Pergamon Press, Oxford, 1961.

[4] M. YORINAGA: On a congruencial property of Fibonacci numbers——Numerical experiments——, Math. J. Okayama Univ. **19**, 5—9.

DEPARTMENT OF MATHEMATICS,
OKAYAMA UNIVERSITY

(*Received December 1, 1976*)