ON PRIMES AND PSUEDO-PRIMES RELATED TO THE FIBONACCI SEQUENCE

EDWARD A. PARBERRY
Pennsylvania State University, State College, Pennsylvania

The two sequences $\{U_n\}$ and $\{V_n\}$ which satisfy the recurrence relation $f(n + 1) = f(n) + f(n - 1)$, and the initial conditions: $J_1 = U_2 = 1$; $V_1 = 1$, $V_2 = 3$; are called the Fibonacci and Lucas sequences, respectively. These sequences have some interesting divisibility properties which are related to the study of prime numbers. For instance, it is well known that every prime number divides infinitely many of the Fibonacci numbers [1, Th. 180, p. 150]; but, although for any particular prime we can give any number of the terms which it divides, we cannot in general give a general rule for finding the least such number. This is the so-called "rank of apparition" problem, where the rank of apparition of a number n, designated by ω_n, is the subscript of the least Fibonacci number which n divides. Wall [2] has shown that a number m divides U_n if and only if ω_m divides N. This property is used frequently in the text without further reference.

The particular divisibility properties with which this paper is concerned are the two "Lucas" equations which hold for all prime $m > 5$ [1, p. 150]:

$$U_{(m-\epsilon_m)} \equiv 0 \pmod{m} \tag{1}$$

$$U_m \equiv \epsilon_m \pmod{m} \quad , \tag{2}$$

where

$$\epsilon_m = \begin{bmatrix} 1 \text{ if } m \equiv \pm 1 \pmod 5 \\ -1 \text{ if } m \equiv \pm 2 \pmod 5 \end{bmatrix}.$$

Clearly it would be nice if (1) and (2) were to hold only for prime m, but this is not the case.

In [3], Emma Lehmer shows that there are infinitely many composite numbers, m, for which (1) is satisfied. She calls these numbers Fibonacci pseudo-primes. Her result is proved here as a special case of Theorem 3, and is extended in Theorem 4 to show that an infinite proper subset of her

pseudo-primes also satisfy (2). For the purpose
a composite number, m, which satisfies both (1) and (2), and which is relatively prime to 30, a strong pseudo-prime.

The main results in the text are as follows:

Theorem 1. Let n be either a prime >5 or a strong pseudo-prime, then:

$$U_{\frac{1}{2}(n-\epsilon_n)} \equiv 0 \pmod{n}, \text{ iff } n \equiv 1 \pmod{4}, \tag{3}$$

$$V_{\frac{1}{2}(n-\epsilon_n)} \equiv 0 \pmod{n}; \text{ iff } n \equiv 3 \pmod{4}. \tag{4}$$

Theorem 2. Let $(n,30) = 1$, and let $m = U_n$, then the following are all equivalent:

$$U_n \equiv \epsilon_n \pmod{n}; \tag{5}$$

$$U_{(m-\epsilon_m)} \equiv 0 \pmod{m}; \tag{6}$$

$$U_{\frac{1}{2}(m-\epsilon_m)} \equiv 0 \pmod{m}; \tag{7}$$

$$U_m \equiv \epsilon_m \pmod{m}. \tag{8}$$

Theorem 3. Let n be a prime >5, or a strong pseudo-prime, then for $m = U_{2n}$,

$$U_{(m-\epsilon_m)} \equiv 0 \pmod{m}; \text{ and } m \text{ is composite.} \tag{9}$$

Remark: Theorem 3 is precisely Emma Lehmer's observation in [3] for n actually prime. However, it was not clear in her proof that the relation depends only on n satisfying (1) and (2), and $(n, 30) = 1$. Theorem 4 now determines those n for which $m = U_{2n}$ satisfies relation (2) as well.

Theorem 4. If $m = U_{2n}$ as in Theorem 3, then m is a strong pseudo-prime if and only if $n \equiv 1,4 \pmod{15}$.

Theorem 1 establishes an identity similar to (1) which gives a further necessary condition for primality (and strong pseudo-primality). This result does not go very far in establishing a set of sufficient conditions, but it has the saving features of determining the parity of the rank of apparition of many primes (Corollaries 1 and 2), and of resolving the conjecture by D. Thoro [4] that no prime of the form $4n + 3$ divides any Fibonacci number with an odd subscript (Corollary 3).

Theorem 5 is the famous Lucas theorem on the primality of Mersenne numbers (numbers of the form $2^p - 1$ where p is a prime $\equiv 3 \pmod 4$). It is included here because Theorem 1 allows a new and elementary proof.

It is obvious [1, p. 150] that U_n is prime only if $n = 4$, or n is prime. Clearly if $m = U_p$ is prime, it must satisfy (1), (2), and (3) when taken as a subscript. However if U_p is not prime, it need not a-priori satisfy any of them. Theorem 2 shows that indeed U_p satisfies all three tests, and in fact that U_p, if not prime, generates an infinite set of strong pseudo-primes recursively.

The following identities are used in the text and may all be found in [2, pp. 148–150].

(10) $$U_n = \frac{\alpha^n - \beta^n}{\sqrt{5}}, \quad \text{where} \quad \alpha = -\beta^{-1} = \frac{1 + \sqrt{5}}{2} \;;$$

(11) $$V_n = \alpha^n + \beta^n \;;$$

(12) $$U_n = (-1)^{n-1}U_{-n}, \quad V_n = (-1)^n V_{-n} \;;$$

(13) (a) $$2^{n-1}U_n = \sum_{k=0}^{\left[\frac{1}{2}(n-1)\right]} \binom{n}{2k+1} 5^k \;;$$

(13) (b) $$2^{n-1}V_n = \sum_{k=0}^{\left[\frac{1}{2}(n-1)\right]} \binom{n}{2k} 5^k \;;$$

(14) $$(U_n, U_{n+1}) = 1, \quad (V_n, V_{n+1}) = 1\ ;$$

(15) $(U_n, V_n) \leq 2$, and equality holds iff $n \equiv 0 \pmod 3$;

(16) $$U_n^2 - U_{n-1}U_{n+1} = (-1)^{n-1}\ ;$$

(17) $$V_n = U_{n+1} + U_{n-1}\ ;$$

Also, in the proof of Theorem 5, we use the following theorem by Lucas [5, p. 302]:

(18) If $\omega_N = N - 1$, or $N + 1$, then N is prime.

Lemma 1. $$U_{a+b} = U_a V_b + (-1)^a U_{b-a}$$

Proof.
$$\begin{aligned} U_a V_b &= \left(\frac{\alpha^a - \beta^a}{\sqrt{5}}\right)(\alpha^b + \beta^b) \\ &= \frac{\alpha^{a+b} - \beta^{a+b} + \alpha^a\beta^b - \alpha^b\beta^a}{\sqrt{5}} \\ &= \frac{\alpha^{a+b} - \beta^{a+b}}{\sqrt{5}} - (\alpha\beta)^a\,\frac{\alpha^{b-a} - \beta^{b-a}}{\sqrt{5}} \\ &= U_{a+b} - (-1)^a U_{b-a} \end{aligned}$$

Lemma 2. (i) $mV_m \equiv U_m \pmod 5$;

(ii) $U_m \equiv m \pmod 5$, if $m \equiv 1 \pmod 4$;

(iii) $U_m \equiv -m \pmod 5$, if $m \equiv 3 \pmod 4$;

(iv) $U_m \equiv -\frac{1}{2}m \pmod 5$, if $m \equiv 0 \pmod 4$;

(v) $U_m \equiv \frac{1}{2}m \pmod 5$, if $m \equiv 2 \pmod 4$.

Proof. From (13),

$$2^{n-1}U_n = \sum_{k=0}^{\left[\frac{1}{2}(n-1)\right]} \binom{n}{2k+1} 5^k \equiv n \pmod 5 \tag{19}$$

and

$$2^{n-1}V_n = \sum_{k=0}^{\left[\frac{1}{2}(n-1)\right]} \binom{n}{2k} 5^k \equiv 1 \pmod 5 \tag{20}$$

Multiplying (19) and (20), and dividing out 2^{n-1}, we get (i). From Fermat's theorem, $2^{4n} \equiv 1 \pmod 5$, $2^{4n+1} \equiv 2 \pmod 5$, etc., and the other relations follow since $(2,5) = 1$.

Theorem 1. Let n be either a prime > 5 or a strong pseudo-prime. then

$$U_{\frac{1}{2}(n-\epsilon_n)} \equiv 0 \pmod n \quad \text{iff} \quad n \equiv 1 \pmod 4 \tag{3}$$

$$V_{\frac{1}{2}(n-\epsilon_n)} \equiv 0 \pmod n \quad \text{iff} \quad n \equiv 3 \pmod 4 \tag{4}$$

Proof. In Lemma 1, let

$$a = \frac{1}{2}(n - \epsilon_n), \quad b = \frac{1}{2}(n + \epsilon_n),$$

then by Eq. (2),

$$U_n = U_{\frac{1}{2}(n-\epsilon_n)} V_{\frac{1}{2}(n+\epsilon_n)} + (-1)^{\frac{1}{2}(n-\epsilon_n)} U_{\epsilon_n} \equiv \epsilon_n \pmod n \tag{21}$$

now

$$U_1 = U_{-1} = 1, \quad \text{and} \quad (-1)^{\frac{1}{2}(n-\epsilon_n)} \equiv \epsilon_n \pmod n \text{ iff } n \equiv 1 \pmod 4.$$

Hence

$$(22) \qquad U_{\frac{1}{2}(n-\epsilon_n)} V_{\frac{1}{2}(n+\epsilon_n)} \equiv 0 \pmod{n} \quad \text{iff} \quad n \equiv 1 \pmod{4} .$$

Also, from (1),

$$(23) \qquad U_{(n-\epsilon_n)} = U_{\frac{1}{2}(n+\epsilon_n)} V_{\frac{1}{2}(n-\epsilon_n)} \equiv 0 \pmod{n} .$$

Now suppose $n \equiv 1 \pmod 4$, and the $p^e | n$, while $p^e \nmid U_{\frac{1}{2}(n-\epsilon_n)}$ then from (22),

$$p \,|\, V_{\frac{1}{2}(n+\epsilon_n)}$$

and from (23),

$$p \,|\, V_{\frac{1}{2}(n-\epsilon_n)}$$

which is impossible since by (14),

$$\left(V_{\frac{1}{2}(n+\epsilon_n)},\ V_{\frac{1}{2}(n-\epsilon_n)}\right) = 1 .$$

Hence

$$n \,|\, U_{\frac{1}{2}(n-\epsilon_n)} \quad \text{iff} \quad n \equiv 1 \pmod 4 ,$$

which proves (3).

If, on the other hand, $n \equiv 3 \pmod 4$; then (21) shows that $p|n$ implies

$$U_{\frac{1}{2}(n-\epsilon_n)} V_{\frac{1}{2}(n+\epsilon_n)} \equiv \pm 2 \pmod{p} .$$

Therefore

$$\left(U_{\frac{1}{2}(n-\epsilon_n)},\ n\right) = 1 ;$$

hence from (23),

$$n \,\Big|\, V_{\frac{1}{2}(n-\epsilon_n)} .$$

And finally if $n \equiv 1 \pmod 4$, then $n \,\Big|\, U_{\frac{1}{2}(n-\epsilon_n)}$; and since

$$\left(U_{\frac{1}{2}(n-\epsilon_n)}, V_{\frac{1}{2}(n-\epsilon_n)}\right) \le 2, \quad n \not\Big|\, V_{\frac{1}{2}(n-\epsilon_n)} ,$$

Corollary 1. If $p \equiv 3 \pmod 4$, then ω_p is even.

Proof. This follows from (1) and Theorem 1, since $\omega_p \mid p - \epsilon_p$ which is even, but $\omega_p \nmid \frac{1}{2}(p - \epsilon_p)$.

Corollary 2. If $p \equiv 13, 17 \pmod{20}$, then ω_p is odd.

Proof. Here $\epsilon_p = -1$, $p \equiv 1 \pmod 4$, hence $\frac{1}{2}(p - \epsilon_p)$ is odd. Therefore, since

$$p \,\Big|\, U_{\frac{1}{2}(p-\epsilon_p)} \quad \text{implies} \quad \omega_p \,\Big|\, \frac{1}{2}(p - \epsilon_p) ,$$

ω_p is odd.

Corollary 3. (Thoro [3]) If $p \mid U_{(2n+1)}$, then $p \not\equiv 3 \pmod 4$.

Proof. $p \mid U_{2n+1}$ implies $\omega_p \mid 2n + 1$ which in turn implies $p = 2$, or $p \equiv 1 \pmod 4$ by Corollary 1.

Theorem 2. Let $(n, 30) = 1$, and let $m = U_n$. Then the following are all equivalent:

(5) (a) $$U_n \equiv \epsilon_n \pmod n ;$$

(6) (b) $$U_{(m-\epsilon_m)} \equiv 0 \pmod m ;$$

(7) (c) $$U_{\frac{1}{2}(m-\epsilon_m)} \equiv 0 \pmod m ;$$

(8) (d) $$U_m \equiv \epsilon_m \pmod m .$$

Proof. (a)$\Longleftrightarrow$(b) .

From Lemma 2, we see that $U_n = m \equiv \pm n \pmod 5$, since n is odd. Therefore $\epsilon_m = \epsilon_n$, and replacing ϵ_n in (a), we have

$$n \mid U_n - \epsilon_m \Leftrightarrow U_n \mid U_{U_n - \epsilon_m} = U_{m-\epsilon_m} .$$

(b) $\Leftrightarrow$ (c)

Since n is odd, and U_n is odd (since $3 \nmid n$) we have:

$$U_n = m \mid U_{m-\epsilon_m} \Leftrightarrow n \mid m - \epsilon_m \Leftrightarrow n \mid \tfrac{1}{2}(m - \epsilon_m) \Leftrightarrow U_n = m \mid U_{\frac{1}{2}(m-\epsilon_m)} .$$

(c) $\Rightarrow$ (d)

Using Lemma 1, we have

$$(24) \quad U_m = U_{\frac{1}{2}(m-\epsilon_m)} V_{\frac{1}{2}(m+\epsilon_m)} + (-1)^{\frac{1}{2}(m-\epsilon_m)} \equiv (-1)^{\frac{1}{2}(m-\epsilon_m)} \pmod{m} .$$

Now since n is odd, we see by Corollary 3, that

$$U_n = m \equiv 1 \pmod{4} .$$

Hence

$$(-1)^{\frac{1}{2}(m-\epsilon_m)} = \epsilon_m .$$

(d) $\Rightarrow$ (c)

Comparing (d) with (24), we see that

$$(25) \qquad U_{\frac{1}{2}(m-\epsilon_m)} V_{\frac{1}{2}(m+\epsilon_m)} \equiv 0 \pmod{m} ,$$

and from (16), we see that

$$U_m^2 - U_{m-\epsilon_m} U_{m+\epsilon_m} = (-1)^{m-1} \equiv 1 \pmod{m} ,$$

hence

$$(26) \qquad U_{m-\epsilon_m} U_{m+\epsilon_m} \equiv 0 \pmod{m} .$$

Now suppose $p^e \mid m$, and $p^e \nmid U_{\frac{1}{2}(m-\epsilon_m)}$, then $p \mid V_{\frac{1}{2}(m+\epsilon_m)}$ by (25). Also $\omega_{p^e} \mid n$ and is therefore odd, hence

$$\omega_{p^e} \nmid \tfrac{1}{2}(m - \epsilon_m) \Rightarrow \omega_{p^e} \nmid m - \epsilon_m \Rightarrow p^e \nmid U_{m-\epsilon_m} .$$

Therefore, Eq. (26) implies that $p \mid U_{m+\epsilon_n}$. But ω_p is also odd, hence

$$\omega_p \mid m + \epsilon_m \Rightarrow \omega_p \,\Big|\, \tfrac{1}{2}(m + \epsilon_m) \Rightarrow p \,\Big|\, U_{\frac{1}{2}(m+\epsilon_m)} ,$$

which is a contradiction since

$$\left(U_{\frac{1}{2}(m+\epsilon_m)}, V_{\frac{1}{2}(m+\epsilon_m)}\right) \le 2 .$$

Hence

$$p^e \mid m \Rightarrow p^e \,\Big|\, U_{\frac{1}{2}(m-\epsilon_m)} ,$$

which means that

$$m \,\Big|\, U_{\frac{1}{2}(m-\epsilon_m)} . \quad \text{Q.E.D.}$$

Theorem 3. Let n be a prime > 5, or a strong pseudo-prime, then for $m = U_{2n}$,

$$U_{(m-\epsilon_m)} \equiv 0 \pmod{m} ;$$

and m is composite.

Proof. We note that $U_{2n} = U_n V_n$ by Lemma 1, and is therefore composite for $n > 2$.

Now, using (2) and (17):

$$U_{2n} \equiv U_n V_n \equiv \epsilon_n V_n \equiv \epsilon_n (U_{n+\epsilon_n} + U_{n-\epsilon_n}) \pmod{n} ,$$

and using (1), and Lemma 1:

$$U_{2n} \equiv \epsilon_n\left(U_{(n+\epsilon_n)}\right) \equiv \epsilon_n\left(U_n V_{\epsilon_n} + (-1)^n U_{-(n-\epsilon_n)}\right)$$

$$\equiv \epsilon_n^2 V_{\epsilon_n} \equiv V_{\epsilon_n} \equiv \epsilon_n \pmod{n} \quad .$$

Hence, $n \mid m - \epsilon_n$; which, since n and m are odd, implies:

$$2n \mid m - \epsilon_n \Rightarrow U_{2n} = m \mid U_{(m-\epsilon_n)} \quad . \tag{27}$$

To complete the proof, we note that by Lemma 2,

$$U_{2n} = m \equiv \pm n \pmod{5}, \text{ hence } \epsilon_m = \epsilon_n \; .$$

Theorem 4. If $m = U_{2n}$ as in Theorem 3, then m is a strong pseudo-prime if and only if $n \equiv 1, 4 \pmod{15}$.

Proof. From Theorem 3, and Lemma 1,

$$U_m = U_{\frac{1}{2}(m-\epsilon_m)} V_{\frac{1}{2}(m+\epsilon_m)} + (-1)^{\frac{1}{2}(m-\epsilon_m)} U_{\epsilon_m} \quad .$$

Now if $m \equiv \epsilon_m \pmod{4}$, then $2n \mid \frac{1}{2}(m - \epsilon_m)$ by (27); hence:

$$U_m \equiv (-1)^{\frac{1}{2}(m-\epsilon_m)} U_{\epsilon_m} \equiv 1 \pmod{m} \; .$$

On the other hand, if $m \equiv -\epsilon_m \pmod{4}$, then a new application of Lemma 1 gives:

$$U_m = U_{\frac{1}{2}(m-2n-\epsilon_m)} V_{\frac{1}{2}(m+2n+\epsilon_m)} + (-1)^{\frac{1}{2}(m-2n-\epsilon_m)} U_{2n+\epsilon_m} \; ;$$

which shows, since now $2n \mid \frac{1}{2}(m - 2n - \epsilon_m)$, that

$$U_m \equiv U_{2n+\epsilon_m} \equiv U_{2n-\epsilon_m} \not\equiv \pm 1 \pmod{m} \; ,$$

hence $U_m \equiv \epsilon_m \pmod{m}$ iff $\epsilon_m = 1$ and $m \equiv 1 \pmod{4}$. This corresponds to $n \equiv \pm 1 \pmod{5}$, and $n \equiv 1 \pmod{3}$ (i.e., $n \equiv 1, 4 \pmod{15}$). Q.E.D.

Theorem 5. (Lucas [5, p. 310]) Let $p \equiv 3 \pmod{4}$ be a prime, then $N = 2^p - 1$ is a prime if and only if $V_{2^{(p-1)}} \equiv 0 \pmod{N}$.

Remark. This is the simplest test of primality known; since

$$V_{2^n} = V^2_{2^{(n-1)}} - 2 ,$$

and hence can be calculated in only n steps.

Proof. Sufficiency:

Let

$$V_{2^{(p-1)}} \equiv 0 \pmod{N} ,$$

then by Lemma 1,

$$U_{2^p} = U_{2^{(p-1)}} V_{2^{(p-1)}} \equiv 0 \pmod{N} = \omega_N \mid 2^p .$$

and since

$$\left(U_{2^{(p-1)}}, V_{2^{(p-1)}}\right) = 1, \ \omega_N = 2^p ;$$

which by (18) gives that N is prime.

Necessity:

Let N be prime, and then since $N \equiv 3 \pmod{4}$, we have by Theorem 1,

$$N \mid V_{\frac{1}{2}(N-\epsilon_N)} ,$$

and since

$$2^p - 1 \equiv 2^3 - 1 \equiv 2 \pmod{5} ,$$

$\epsilon_N = -1$. Therefore, $N \mid V_{2^{(p-1)}}$. Q.E.D.

REFERENCES

1. G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, Oxford University Press, 4th Ed., 1960.
2. D. D. Wall, "Fibonacci Series Modulo m," Amer. Math. Monthly, 67 (1960).
3. E. Lehmer, "On the Infinitude of Fibonacci Pseudo-Primes," Fibonacci Quarterly, October, 1964, p. 229.
4. D. Thoro, "Two Fibonacci Conjectures," Fibonacci Quarterly, October, 1965, p. 186.
5. E. Lucas, "Theorie der Fonctions Numeriques Simplement Periodiques," Amer. J. of Math., Vol. 1, Baltimore, 1878.

* * * * *

[Continued from page 48.]

3. F. B. Hildebrand, Methods of Applied Mathematics, Englewood Cliffs, Prentice-Hall, Inc., 1961, pp. 227-249.
4. James A. Jeske, "Linear Recurrence Relations, Part I," Fibonacci Quarterly, Vol. 1, No. 2, April 1965, p. 69.
5. Kenneth S. Miller, An Introduction to the Calculus of Finite Differences and Difference Equations, New York, Henry Holt and Co., 1960, pp. 126-157.
6. George Ledin, Jr., "On a Certain Kind of Fibonacci Sums," Fibonacci Quarterly, Vol. 5, No. 1, Feb., 1967, pp. 45-58.
7. R. J. Weinshenk, "Convolutions and Difference Equations Associated with the N-Reflections of Light in two Glass Plates," San Jose State College Masters Thesis, June, 1965.
8. J. A. H. Hunter, Problem H-48 with solution in Vol. 3, No. 4, p. 303, Fibonacci Quarterly.
9. Brother U. Alfred, "Summation of $\sum_{k=1}^{n} k^m F_{k+r}$ Finite Difference Approach," Fibonacci Quarterly, Vol. 5 (19672, pp. 91-98.
10. David Zeitlin, "On Summation Formulas and Identities for Fibonacci Numbers," Fibonacci Quarterly, Vol. 5 (1967), pp. 1-43.

* * * * *