DIVISIBILITY PROPERTIES OF FIBONACCCI POLYNOMIALS

W. A. WEBB and E. A. PARBERRY
Pennsylvania State University, State College, Pennsylvania

1. INTRODUCTION

A famous unsolved problem in number theory asks the question, "Are there infinitely many prime numbers in the Fibonacci sequence?" It is well known that if $\{U_n\}$ is the sequence defined by:

$$U_n = U_{n-1} + U_{n-2}; \quad U_0 = 0, \quad U_1 = 1,$$

then U_n is prime only if n is prime. The converse, however, is not true since, for example, $U_{19} = 113 \cdot 37$. Whether there are infinitely many primes p such that U_p is prime, or indeed whether there are infinitely many exceptions, has been an elusive problem for over a century.

In this paper we parametrize the sequence by using the recursion:

$$U_n(x) = xU_{n-1}(x) + U_{n-2}(x); \quad U_0(x) = 0, \quad U_1(x) = 1 .$$

(Note that $U_n(1) = U_n$.) The resulting sequence: $0, 1, x, x^2 + 1, x^3 + 2x, x^4 + 3x^2 + 1$, etc., satisfies all of the important divisibility relations of the original sequence with the following welcome exception:

Theorem 1. $U_n(x)$ is irreducible if and only if n is prime, which we will prove here.

The following notation will be used throughout the paper.

$$\omega = \frac{x + \sqrt{x^2 + 4}}{2}, \qquad \overline{\omega} = \frac{x - \sqrt{x^2 + 4}}{2}$$

$$V_n(x) = xV_{n-1}(x) + V_{n-2}(x); \quad V_0(x) = 2, \quad V_1(x) = x .$$

2. SOME PROPERTIES OF THE SEQUENCE

The following are just a few of the results concerning the sequence which may be readily proved.

(1) $$U_n(x) = \frac{\omega^n - \bar{\omega}^n}{\omega - \bar{\omega}} .$$

(2) $$\omega\bar{\omega} = -1 .$$

(3) $$V_n(x) = \omega^n + \bar{\omega}^n .$$

(4) $$U_n(x) \mid U_{nm}(x)$$

If

$$U_n(x) = \sum_{m=0}^{\left[\frac{n-1}{2}\right]} \Delta(n,m)x^{n-2m-1} ,$$

then,

(5) $$\Delta(n,m) = \frac{4^m}{2^{n-1}} \sum_{j=m}^{\left[\frac{n-1}{2}\right]} \binom{n}{2j+1}\binom{j}{m} = \binom{n-m-1}{m} .$$

(6)
i) $$U_{2n+1}(x) \equiv (-1)^n(2n+1) \pmod{(x^2+4)} ;$$
ii) $$U_{2n}(x) \equiv (-1)^{n-1} nx \pmod{(x^2+4)} .$$

(7)
i) $$U_{a+b}(x) = U_a(x)V_b(x) - (-1)^b U_{a-b}(x)$$
ii) $$U_{a+b}(x) = U_b(x)V_a(x) + (-1)^b U_{a-b}(x) .$$

(8) $$(U_a(x), U_b(x)) = U_{(a,b)}(x) .$$

If p is a prime,

(9) $$U_p(x) \equiv (x^2+4)^{\frac{p-1}{2}} \pmod{p} .$$

Equations (1), (2), and (3) are well known, and (4) follows immediately from (1). Equation (5) follows from (1) by expanding and comparing coefficients, while (6) and (7) may be proved by routine calculation using (1), (2), and (3). To prove (8), let

$$I = \{n : f(x) \mid U_n(x)\} \quad ,$$

where

$$f(x) = (U_a(x),\ U_b(x)) \ .$$

If $r \in I$, then by (4) $mr \in I$ for any integer m. If $r \in I$ and $t \in I$, then by (7), $r - t \in I$. Hence I is an ideal containing a and b, and therefore $(a,b) \in I$, which shows that

$$(U_a(x),\ U_b(x)) \mid U_{(a,b)}(x) \quad ,$$

and by (4) we have

$$U_{(a,b)}(x) \mid (U_a(x),\ U_b(x)) \ .$$

The proof of the identity in (9) goes as follows.

By (5) we have,

$$\Delta(p,m) \equiv \binom{\frac{p-1}{2}}{m} 4^m \pmod{p} \quad ,$$

hence

$$U_p(x) \equiv \sum_{m=0}^{\frac{p-1}{2}} \binom{\frac{p-1}{2}}{m} x^{2\left(\frac{p-1}{2}-m\right)} 4^m \equiv (x^2+4)^{\frac{p-1}{2}} \pmod{p} \ .$$

3. PROOF OF THEOREM 1

That $U_n(x)$ is irreducible only if n is prime, follows immediately from (8). We now prove that $U_p(x)$ is always irreducible.

Suppose that for some odd prime, p, $U_p(x)$ is reducible. Then we may write

$$U_p(x) = \prod_{i=1}^{m} f_i(x) ,$$

where the $f_i(x)$ are all monic irreducibles.

Case 1. $m \geq 3$. Since $U_p(x)$ contains only even powers of x, $U_p(x) = U_p(-x)$. Hence for each i there exists a j such that $f_i(x) = \pm f_j(-x)$, and for that same j, $f_i(-x) = \pm f_j(x)$. Therefore,

$$f_i(x)f_j(x) = (\pm f_j(-x))(\pm f_i(-x)) = f_i(-x)f_j(-x) .$$

Hence if $i \neq j$, $U_p(x)$ is divisible by an even polynomial. On the other hand, if $i = j$, $f_i(x)$ is even since $f_i(0) \neq 0$. In either instance, we have some factorization $h(x)g(x) = U_p(x)$, where $h(x)$ and $g(x)$ have degree ≥ 2 and both are even functions of x. Now by the division algorithm, we may write

$$h(x) = \ell_1(x)(x^2 + 4) + h ,$$

and

$$g(x) = \ell_2(x)(x^2 + 4) + g ,$$

where h and g are integers. Now by (6), we see that

$$h(x)g(x) \equiv \pm p \pmod{x^2 + 4} ,$$

hence $h = \pm p$ and $g = \pm 1$ without loss of generality. On the other hand, by (9), we have

$$g(x) \equiv (x^2 + 4)^k \pmod{p} \quad \text{when} \quad p \equiv 3 \bmod 4 ,$$

and

$$g(x) \equiv (x + \alpha)^{k_1}(x - \alpha)^{k_2} \pmod{p} \quad \text{when} \quad p \equiv 1 \mod 4,$$

where $\alpha = 2\sqrt{-1} \bmod p$. In the second case, we note that $k_1 = k_2$ since $g(x) = g(-x) \pmod{p}$. Hence, in either instance, we may write

$$g(x) = \ell_3(x)p + (x^2 + 4)^k ,$$

where $\ell_3(x)$ is even since $g(x)$ and $(x^2 + 4)$ are. Therefore $\ell_3(x) \equiv c \pmod{x^2 + 4}$ for some integer c, and we have

$$\pm 1 \equiv g(x) \equiv cp \pmod{x^2 + 4} ,$$

a contradiction. Hence if $U_p(x)$ is reducible, it must have only two factors.

Case 2. $m = 2$. Let $U_p(x) = f(x)g(x)$ where $f(x)$ and $g(x)$ are irreducible and monic. Now either $f(-x) = f(x)$ or $f(-x) = g(x)$. (Note: since $\operatorname{sgn} f(0) - \operatorname{sgn} g(0) \neq 0$, $f(-x) \neq -f(x)$ or $-g(x)$). If $f(-x) = f(x)$, the argument in Case 1 is applicable, since $f(x)$ and $g(x)$ are even. Hence we may assume $f(-x) = g(x)$. Now if $p \equiv 3 \pmod 4$, we get an immediate contradiction. Since

$$\deg f(x) = \deg g(x) = \frac{p - 1}{2} ,$$

which is odd, we have that the leading coefficients of $f(-x)$ and $g(x)$ have opposite signs. Therefore $p \equiv 1 \pmod 4$. Now if we let

$$f(x) = \sum_{n=0}^{\frac{p-1}{2}} a_n x^{\frac{p-1}{2}-n} \quad \text{and} \quad g(x) = \sum_{n=0}^{\frac{p-1}{2}} (-1)^n a_n x^{\frac{p-1}{2}-n} ,$$

then we have

$$f(x)g(x) = x^{p-1} + (2a_2 - a_1^2)x^{p-3} + (2a_4 - 2a_3a_1 + a_2^2)x^{p-5} + \cdots .$$

Now from (5) we have that $(2a_2 - a_1^2) = p - 2$ which means a_1 must be odd and consequently a_2 is even since $2a_2 \equiv 0 \pmod 4$. But also from (5), we have that

$$(2a_4 - 2a_3a_1 + a_2^2) = \frac{(p - 3)(p - 4)}{2} ,$$

which is odd; this is a contradiction since a_2 is even. Therefore $U_p(x)$ is irreducible.

4. FURTHER CONSIDERATIONS

The generating function for $\{U_n(x)\}$ is quite easy to derive, but not very illuminating for number theoretic purposes. We include it here for the sake of completeness.

Let

$$f(x,y) = \sum_{n=0}^{\infty} U_n(x)y^n ,$$

then

$$f(x,y) = \frac{y}{1 - xy - y^2} ,$$

by using the recursion relation and the fact that $U_n(x) = (-1)^{n-1}U_{-n}(x)$.

The main theorem of this paper brings to mind the sequence of cyclotomic polynomials which are also irreducible for prime numbers. We conclude this paper by showing the following inherent connection between the two sequences.

Theorem. The $n - 1$ roots of $U_n(x)$ are given by

$$U_n\left(2i \cos \frac{k\pi}{n}\right) = 0 ,$$

for $k = 1,2,\cdots,n - 1$.

Proof. Let $x = 2i \cos \theta$, $0 \leq \theta \leq \pi$, then from (1),

$$U_n(2i \cos \theta) = \frac{(i \cos \theta + \sin \theta)^n - (i \cos \theta - \sin \theta)^n}{2 \sin \theta}$$

$$= \frac{(-i)^n (e^{-i\theta n} - e^{i\theta n})}{2 \sin \theta}$$

$$U_n(2i \cos \theta) = \frac{(i)^{n-1} \sin n\theta}{\sin \theta}$$

which is zero for

$$\theta = \frac{k\pi}{n}, \quad k = 1, 2, \cdots, n - 1.$$

* * * * *

[Continued from page 456.]

$$|\alpha_i|^{\frac{m+r}{r}},$$

and the circle about $(1,0)$ with radius $|\alpha_i|$. Now, for $\alpha_i = \alpha$, the two circles must be tangent externally (tangent, because $1 - \alpha$ is real; and externally, since $0 < 1 - \alpha < 1$). Now if there exists an i such that $|\alpha_i| < \alpha$, then the radii of both circles would be smaller, and hence they couldn't intersect. This shows that $\alpha = \alpha_i$.

* * * * *