DIVISIBILITY PROPERTIES OF GENERALIZED FIBONACCI POLYNOMIALS

VERNER E. HOGGATT, JR.
San Jose State University, San Jose, California 95192
and
CALVIN T. LONG
Washington State University, Pullman, Washington 99163

1. INTRODUCTION

In [2], Webb and Parberry study the divisibility properties of the Fibonacci polynomial sequence $\{f_n(x)\}$ defined by the recursion

$$f_{n+2}(x) = xf_{n+1}(x) + f_n(x); \qquad f_0(x) = 0, \quad f_1(x) = 1.$$

As one would expect, these polynomials possess many properties of the Fibonacci sequence which, of course, is just the integral sequence $\{f_n(1)\}$. However, a most surprising result is that $f_p(x)$ is irreducible over the ring of integers if and only if p is a prime. In contrast, for the Fibonacci sequence, the condition that n be a prime is necessary but not sufficient for the primality of $f_n(1) = F_n$. For instance, $F_{19} = 4181 = 37 \cdot 113$.

In the present paper, we obtain a series of results including that of Webb and Parberry for the more general but clearly related sequence $\{u_n(x,y)\}$ defined by the recursion

$$u_{n+2}(x,y) = xu_{n+1}(x,y) + yu_n(x,y); \qquad u_0(x,y) = 0, \quad u_1(x,y) = 1.$$

The first few terms of the sequence are as shown in the following table:

n	$u_n(x,y)$
0	0
1	1
2	x
3	$x^2 + y$
4	$x^3 + 2xy$
5	$x^4 + 3x^2y + y^2$
6	$x^5 + 4x^3y + 3xy^2$
7	$x^6 + 5x^4y + 6x^2y^2 + y^3$
8	$x^7 + 6x^5y + 10x^3y^2 + 4xy^3$
...	...

The basic fact that we will need is that $Z[x,y]$, the ring of polynomials over the integers, is a unique factorization domain. Thus, the greatest common divisor of two elements in $Z[x,y]$ is (essentially uniquely) defined.

Useful Property A: if α, β, and γ are in $Z[x,y]$ and $\gamma \mid \alpha\beta$ with γ irreducible, then $\gamma \mid \alpha$ or $\gamma \mid \beta$.

For simplicity, we will frequently use u_n in place of $u_n(x,y)$ and will let

$$\alpha = \alpha(x,y) = \frac{x + \sqrt{x^2 + 4y}}{2}$$

and

$$\beta = \beta(x,y) = \frac{x - \sqrt{x^2 + 4y}}{2} .$$

2. BASIC PROPERTIES OF THE SEQUENCE

Again, as one would expect, many properties of the Fibonacci sequence hold for the present sequence. In particular, the following two results are entirely expected and are easily proved by induction.

Theorem 1. For $n \geq 0$,

$$u_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} .$$

Theorem 2. For $m \geq 0$ and $n \geq 0$,

$$u_{m+n+1} = u_{m+1}u_{n+1} + yu_m u_n .$$

The next result that one would expect is that $(u_n, u_{n+1}) = 1$ for $n \geq 0$. To obtain this we first prove the following lemma.

Lemma 3. For $n > 0$, $(y, u_n) = 1$.

Proof. The assertion is clearly true for $n = 1$ since $u_1 = 1$. Assume that it is true for any fixed integer $k \geq 1$. Then, since

$$u_{k+1} = xu_k + yu_{k-1} ,$$

the assertion is also true for $n = k + 1$, and hence for all $n \geq 1$ as claimed.

We can now prove

Theorem 4. For $n \geq 0$, $(u_n, u_{n+1}) = 1$.

Proof. Again the result is trivially true for $n = 0$ and $n = 1$ since $u_0 = 0$, $u_1 = 1$, and $u_2 = x$. Assume that it is true for $n = k - 1$ where k is any fixed integer, $k \geq 2$, and let $d(x,y) = (u_k, u_{k+1})$. Since

$$u_{k+1} = xu_k + yu_{k-1} ,$$

this implies that $d(x,y) \mid u_{k-1}y$. But $(d(x,y), y) = 1$ by Lemma 3 and so $d(x,y) \mid u_{k-1}$. But then $d(x,y) \mid 1$ since $(u_{k-1}, u_k) = 1$ and the desired result holds for all $n \geq 0$ as claimed.

Lemma 5. For $n \geq 0$,

$$u_n(x,y) = \sum_{i=0}^{[(n-1)/2]} \binom{n-i-1}{i} x^{n-2i-1} y^i .$$

Proof. We define the empty sum to be zero, so the result holds for $n = 0$. For $n = 1$, the sum reduces to the single term

$$\binom{0}{0} x^0 y^0 = 1 = u_1 .$$

Assume that the claim is true for $n = k - 1$ and $n = k$, where $k \geq 1$ is fixed. Then

$$\begin{aligned} u_{k+1} &= xu_k + yu_{k-1} \\ &= \sum_{i=0}^{[(k-1)/2]} \binom{k-i-1}{i} x^{k-2i} y^i + \sum_{i=0}^{[(k-2)/2]} \binom{k-i-2}{i} x^{k-2i-2} y^{i+1} \\ &= \sum_{i=0}^{[(k-1)/2]} \binom{k-i-1}{i} x^{k-2i} y^i + \sum_{i=0}^{[k/2]} \binom{k-i-1}{i-1} x^{k-2i} y^i \\ &= \sum_{i=0}^{[k/2]} \binom{k-i}{i} x^{k-2i} y^i . \end{aligned}$$

Thus, the result holds for $n = k + 1$ and hence also for all $n \geq 0$ as claimed.

3. THE PRINCIPAL THEOREMS

Theorem 6. For $m \geq 2$, $u_m \mid u_n$ if and only if $m \mid n$.

Proof. Clearly $u_m \mid u_m$. Now suppose that $u_m \mid u_{km}$ where $k \geq 1$ is fixed. Then, using Theorem 2,

$$\begin{aligned} u_{(k+1)m} &= u_{km+m} \\ &= u_{km}u_{m+1} + yu_{km-1}u_m \ . \end{aligned}$$

But, since $u_m \mid u_{km}$ by the induction assumption, this clearly implies that $u_m \mid u_{(k+1)m}$. Thus, $u_m \mid u_n$ if $m \mid n$.

Now suppose that $m \geq 2$ and that $u_m \mid u_n$. If $m \nmid n$, then there exist integers q and r with $0 < r < m$, such that $n = mq + r$. Again by Theorem 2, we have that

$$\begin{aligned} u_n &= u_{mq+r} \\ &= u_{mq+1}u_r + yu_{mq}u_{r-1} \ . \end{aligned}$$

Since $u_m \mid u_{mq}$ by the first part of the proof, this implies that $u_m \mid u_{mq+1}u_r$. But, since $(u_{mq}, u_{mq+1}) = 1$ by Theorem 4, this implies that $u_m \mid u_r$ and this is impossible, since u_r is of lower degree than u_m in x. Therefore, $r = 0$ and $m \mid n$ and the proof is complete.

Theorem 7. For $m \geq 0$, $n \geq 0$, $(u_m, u_n) = u_{(m,n)}$.

Proof. Let $d = d(x,y) = (u_m, u_n)$. Then it is immediate from Theorem 6 that $u_{(m,n)} \mid d$.

Now, it is well known that there exist integers r and s with, say, $r > 0$ and $s < 0$, such that

$$(m,n) = rm + sn \ .$$

Thus, by Theorem 2,

$$\begin{aligned} u_{rm} &= u_{(m,n)+(-s)n} \\ &= u_{(m,n)}u_{-sn+1} + yu_{(m,n)-1}u_{-sn} \ . \end{aligned}$$

But then $d \mid u_{-sn}$ and $d \mid u_{rm}$ by Theorem 6 and so $d \mid u_{(m,n)}u_{-sn+1}$. But, $(d, u_{-sn+1}) = 1$ by Theorem 4, and so $d \mid u_{(m,n)}$ by Useful Property A from Section 1. Thus, $d = u_{(m,n)}$ as claimed.

Theorem 8. The polynomial $u_n = u_n(x,y)$ is irreducible over the rational field Q if and only if n is a prime.

Proof. From Lemma 5, if we replace y by y^2 we have

$$u_n(x,y^2) = \sum_{i=0}^{[(n-1)/2]} \binom{n-i-1}{i} x^{n-2i-1} y^{2i}$$

which is clearly homogeneous of degree $n - 1$. Now it is well known (see, for example, [1, p. 376, problem 5]) that a homogeneous polynomial $f(x,y)$ over a field F is irreducible if and only if the corresponding polynomial $f(x,1)$ is irreducible over F. Since $u_n(x,1)$ is irreducible by Theorem 1 of [2], it follows that $u_n(x,y^2)$ and hence also $u_n(x,y)$ is irreducible over the rational field and thus is irreducible over the integers.

4. SOME ADDITIONAL THEOREMS

For the Fibonacci sequence $\{F_n\}$, for any nonzero integer r there always exists a positive integer m such that $r \mid F_m$. Also, if m is the least positive integer such that $r \mid F_m$, then $r \mid F_n$ if and only if $m \mid n$. It is natural to seek the analogous results for the sequence of Fibonacci polynomials $\{f_n(x)\}$ considered by Webb and Parberry and the generalized sequence $\{u_n(x,y)\}$ considered here. In a sense, the first problem is solved by Webb and Parberry for the sequence of Fibonacci polynomials, since they give explicitly the roots of each such polynomial. However, it is still not clear exactly which polynomials $r(x)$ possess the derived property. On the other hand, it is immediate that the first result mentioned above does not hold for all polynomials $r(x)$. For example, if c is positive, no linear factor $x - c$ can divide any $f_n(x)$ since this would imply that $f_n(c) = 0$, and this is impossible since $f_n(x)$ has only positive coefficients.

Along these lines, we offer the following theorems which, among other things, show that the second property mentioned above does hold without change for $u_n(x,y)$ and hence also for $f_n(x)$. We give this result first.

Theorem 9. Let $r = r(x,y)$ be any polynomial in x and y. If there exists a least positive integer m such that $r \mid u_m$, then $r \mid u_n$ if and only if $m \mid n$.

Proof. By Theorem 6, if $m \mid n$, then $u_m \mid u_n$. Therefore, if $r \mid u_m$ we have by transitivity that $r \mid u_n$. Now suppose that $r \mid u_n$ and yet $m \nmid n$. Then there exist integers q and s with $0 < s < m$ such that $n = mq + s$. Therefore, by Theorem 2,

$$\begin{aligned} u_n &= u_{mq+s} \\ &= u_{mq+1}u_s + yu_{mq}u_{s-1} . \end{aligned}$$

Since $r \mid u_{mq}$ and $r \mid u_n$, it follows that $r \mid u_{mq+1}u_s$. But $(u_{mq}, u_{mq+1}) = 1$ and this implies that $r \mid u_s$. But this violates the minimality condition on m and so the proof is complete.

Theorem 10. For $n \geq 2$,

$$u_n(x,y) = \prod_{k=1}^{n-1}\left(x - 2i\sqrt{y}\cos\frac{k\pi}{n}\right) .$$

Proof. From the proof of Theorem 8, it follows that

$$u_n(x,y^2) = y^{n-1}u_n\left(\frac{x}{y}, 1\right) = y^{n-1}f_n\left(\frac{x}{y}\right) ,$$

where $f_n(x)$ is the n^{th} Fibonacci polynomial mentioned above. Thus,

$$u_n(x,y) = y^{(n-1)/2}f_n(x/\sqrt{y})$$

and it follows from [2, page 462] that

$$f_n(x/\sqrt{y}) = \prod_{k=1}^{n-1}\left(\frac{x}{\sqrt{y}} - 2i\cos\frac{k\pi}{n}\right) .$$

This, with the preceding equation, immediately yields the desired result.

Corollary 10. For $n \geq 2$, n even,

$$u_n(x,y) = x\prod_{k=1}^{(n-2)/2}\left(x^2 + 4y\cos^2\frac{k\pi}{n}\right)$$

and, for n odd,

$$u_n(x,y) = \prod_{k=1}^{(n-1)/2}\left(x^2 + 4y\cos^2\frac{k\pi}{n}\right) .$$

Proof. This is an immediate consequence of Theorem 10, since, for $1 \leq k < n/2$,

$$\cos\frac{k\pi}{n} = -\cos\frac{(n-k)\pi}{n} .$$

It is clear from the preceding theorems that there is a precise correspondence between the polynomial factors of $u_n(x,y)$ and those of $u_n(x,1) = f_n(x)$. Thus, it suffices to consider only those of $f_n(x)$. Also, it is clear that, except for the factor x, the only polynomial factors of $f_n(x)$ with integral coefficients contain only even powers of x. While we are not able to say in every case which even polynomials are factors of some $f_n(x)$ we offer the following partial results.

Theorem 11.

(i) $x \mid f_n(x)$ if and only if n is even.

(ii) $(x^2 + 1) \mid f_n(x)$ if and only if $3 \mid n$.

(iii) $(x^2 + 2) \mid f_n(x)$ if and only if $4 \mid n$.

(iv) $(x^2 + 3) \mid f_n(x)$ if and only if $6 \mid n$.

(v) $(x^2 + c) \nmid f_n(x)$ if $c \neq 1, 2,$ or 3 and c is an integer.

Proof. Since, except for x only, all polynomials with integral coefficients dividing any $f_n(x)$ must be even, the results (i) through (iv) all follow from Theorem 9 with $y = 1$. One has only to observe that $f_2(x)$ is the first Fibonacci polynomial divisible by x, that $f_3(x)$ is the first Fibonacci polynomial divisible by $x^2 + 1$, and so on. Part (v) follows from the fact that $1 \le 4\cos^2\alpha < 4$ for an α in the interval $(0, \pi/2)$.

Theorem 12. Let m be a positive integer and let $N(m)$ denote the number of even polynomials of degree $2m$ and with integral coefficients which divide at least one (and hence infinitely many) members of the sequence $\{f_n(x)\}$. Then

$$N(m) < \prod_{k=1}^{m} \binom{m}{k} 4^k .$$

Proof. Let $f(x)$ be any polynomial counted by $N(m)$. It follows from Corollary 10 with $y = 1$ that

$$\begin{aligned} f(x) &= x^{2m} + a_{m-1}x^{2m-2} + \cdots + a_1x^2 + a_0 \\ &= \prod_{j=1}^{m} (x^2 + \alpha_j) \quad , \end{aligned}$$

where $\alpha_j = 4\cos^2\beta_j$ with $0 < \beta_j < \pi/2$ for each j. Therefore, $0 < \alpha_j < 4$ for each j. Since a_{m-k} is the k^{th} elementary symmetric function of the α_j's, it follows that

$$0 < a_{m-k} < \binom{m}{k} 4^k$$

and hence that

$$N(m) < \prod_{k=1}^{m} \binom{m}{k} 4^k$$

as claimed.

Of course, the estimate in Theorem 12 is exceedingly crude and can certainly be improved. It is probably too much to expect that we will ever know the exact value of $N(m)$ for every m.

Our final theorem shows that with but one added condition the generalization to $u_n(a,b)$ of the first result mentioned in this section is valid.

Theorem 13. Let r be a positive integer with $(r,b) = 1$. Then there exists m such that $r \mid u_m(a,b)$.

Proof. Consider the sequence $u_n(a,b)$ modulo r. Since there exist precisely r^2 distinct ordered pairs (c,d) modulo r, it is clear that the set of ordered pairs

$$\{(u_0(a,b),\ u_1(a,b)),\ (u_1(a,b),\ u_2(a,b)),\ \cdots,\ (u_{r^2}(a,b),\ u_{r^2+1}(a,b))\}$$

must contain at least two identical pairs modulo r. That is, there exist s and t with $0 \le s < t \le r^2$ such that

$$u_s(a,b) \equiv u_t(a,b) \pmod{r}$$

and

$$u_{s+1}(a,b) \equiv u_{t+1}(a,b) \pmod{r} .$$

But

$$bu_{s-1}(a,b) = u_{s+1}(a,b) - au_s(a,b)$$

and

$$bu_{t-1}(a,b) = u_{t+1}(a,b) - au_t(a,b)$$

and this implies that

$$bu_{s-1}(a,b) \equiv bu_{t-1}(a,b) \pmod{r} .$$

Since $(r,b) = 1$, this yields

$$u_{s-1}(a,b) \equiv u_{t-1}(a,b) \pmod{r} .$$

Applying this argument repeatedly, we finally obtain

$$0 = u_{s-s}(a,b) \equiv u_{t-s}(a,b) \pmod{r}$$

so that $r \mid u_{t-s}(a,b)$ and the proof is complete.

REFERENCES

1. S. MacLane and G. Birkhoff, Algebra, The MacMillan Company, New York, N.Y., 1967.
2. W. A. Webb and E. A. Parberry, "Divisibility Properties of Fibonacci Polynomials," Fibonacci Quarterly, Vol. 7, No. 5 (Dec. 1969), pp. 457-463.