THE IRREDUCIBLE FACTORIZATION OF FIBONACCI POLYNOMIALS OVER Q

Dan Levy
The Academic College, 4 Antokolsky St., Tel-Aviv 64044, Israel

(*Submitted June 1999-Final Revision April 2000*)

1. INTRODUCTION

The Lucas sequences, which include the Fibonacci numbers as a special case, arise as solutions to the recursion relation

$$y_{n+1} = ay_n + by_{n-1}, \quad n \geq 1, \tag{1}$$

where a, b and $(y_n)_{n\geq 0}$ take values in some specified ring and a and b are fixed elements which do not depend on the integer index n. A solution $(y_n)_{n\geq 0}$ is completely specified once the values of y_0 and y_1 are given. It is customary to denote by $F_n(a, b)$ the solution corresponding to the choice $y_0 = 0$, $y_1 = 1$, and by $L_n(a, b)$ the solution corresponding to the choice $y_0 = 2$, $y_1 = a$. Loosely speaking, in cases of interest the general solution of (1) can be expressed as a linear combination of these two linearly independent solutions.

Choosing $a = x$ to be an indeterminate and b to be some fixed integer, each of these solutions defines an infinite sequence of polynomials over Z. More specifically, four distinct polynomial sequences of this type will be considered in the present paper, namely, $U_n(x) = F_n(x, 1)$, $V_n(x) = L_n(x, 1)$, $C_n(x) = F_n(x, -1)$, and $D_n(x) = L_n(x, -1)$. The polynomials $U_n(x)$ are known as the Fibonacci polynomials ($U_n(1)$ are the Fibonacci numbers), $V_n(x)$ are termed the Lucas polynomials ($V_n(1)$ are the Lucas numbers), while $C_n(x)$ and $D_n(x)$ are related to the Chebyshev polynomials. Hereinafter, "Fibonacci polynomials" will be used as a collective name for $U_n(x)$, $V_n(x)$, $C_n(x)$, and $D_n(x)$.

The main result of the paper is the prime factorization of the Fibonacci polynomials over the field of rational numbers Q. Webb and Parberry [5] have observed that while $U_n(x)$ enjoy all the well-known divisibility properties of the Fibonacci numbers, they possess a general property which the $U_n(1)$ lack, namely, that $U_p(x)$ is irreducible over Q iff p is a prime. We recall that the prime factorization of $T_n(x) = \sum_{i=0}^{n-1} x^i$ over Q is well known [4] and, in particular, $T_p(x)$ is irreducible over Q iff p is a prime. The irreducible factors are the cyclotomic polynomials $\Phi_m(x)$, which are given by

$$\begin{aligned} \Phi_m(x) &= \prod_{\substack{k=1 \\ \gcd(k,m)=1}}^{m-1} \left(x - e^{i\frac{2\pi k}{m}}\right), \quad m > 1, \\ \Phi_1(x) &= (x-1), \quad m = 1. \end{aligned} \tag{2}$$

The prime factorization of $T_n(x)$ is given by

$$T_n(x) = \prod_{\substack{d|n \\ d>1}} \Phi_d(x), \quad n > 1. \tag{3}$$

Multiplying (3) by $x - 1$ gives the equivalent form

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \quad n \geq 1. \tag{4}$$

Relation (4) can be "inverted" with the help of the Möbius function in order to obtain an explicit expression for the n^{th} cyclotomic polynomial:

$$\Phi_n(x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}, \quad n \geq 1. \tag{5}$$

As we shall see, the structure of the prime factors of the Fibonacci polynomials over Q is similar, and the proof of their irreducibility follows the textbook proof of the irreducibility of the cyclotomic polynomials.

2. RELEVANT PROPERTIES OF FIBONACCI POLYNOMIALS

Let $Q[i]$ denote the field of rational Gaussian numbers, i.e., the quadratic extension of Q by $i = \sqrt{-1}$. Looking at the Fibonacci polynomials over this field, the following relations are easy to establish.

Lemma 1: For all $n \geq 0$, $C_n(x) = i^{n-1}U_n(-ix)$, and $D_n(x) = i^n V_n(-ix)$.

Proof: By induction on n using (1) and the initial conditions. □

The following proposition lists some well-known identities satisfied by the Fibonacci polynomials (for a generalization of some of these identities to $F_n(a,b)$ and $L_n(a,b)$, see [3]).

Proposition 1: Let:

$$w = \frac{x+\sqrt{x^2+4}}{2}, \quad \overline{w} = \frac{x-\sqrt{x^2+4}}{2}, \quad z = \frac{x+\sqrt{x^2-4}}{2}, \text{ and } \overline{z} = \frac{x-\sqrt{x^2-4}}{2}.$$

$$U_n(x) = \frac{w^n - \overline{w}^n}{w - \overline{w}}; \quad C_n(x) = \frac{z^n - \overline{z}^n}{z - \overline{z}}. \tag{6}$$

$$V_n(x) = w^n + \overline{w}^n; \quad D_n(x) = z^n + \overline{z}^n. \tag{7}$$

$$U_n(x) = \sum_{m=0}^{[\frac{n-1}{2}]} \Delta(n,m)x^{n-2m-1} \quad \text{and} \quad C_n(x) = \sum_{m=0}^{[\frac{n-1}{2}]} (-1)^m \Delta(n,m)x^{n-2m-1},$$

where

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

$$V_n(x) = \sum_{m=0}^{[\frac{n}{2}]} \mathrm{E}(n,m)x^{n-2m} \quad \text{and} \quad D_n(x) = \sum_{m=0}^{[\frac{n}{2}]} (-1)^m \mathrm{E}(n,m)x^{n-2m},$$

where

$$\mathrm{E}(n,m) = \frac{4^m}{2^{n-1}} \sum_{j=m}^{[\frac{n}{2}]} \binom{n}{2j}\binom{j}{m} = \binom{n-m}{m} + \binom{n-m-1}{m-1}. \tag{8}$$

$$U_{a+b}(x) = U_a(x)V_b(x) - (-1)^b U_{a-b}(x). \tag{9}$$

$$U_{a+b}(x) = U_b(x)V_a(x) + (-1)^b U_{a-b}(x). \tag{10}$$

$$U_{a+b}(x) = U_{a-1}(x)U_b(x) + U_a(x)U_{b+1}(x). \tag{11}$$
$$C_{a+b}(x) = C_a(x)D_b(x) - C_{a-b}(x). \tag{12}$$
$$C_{a+b}(x) = C_b(x)D_a(x) + C_{a-b}(x). \tag{13}$$
$$C_{a+b}(x) = C_a(x)C_{b+1}(x) - C_{a-1}(x)C_b(x). \tag{14}$$

Proof: Most of the claims concerning $U_n(x)$ and $V_n(x)$ are quoted from Webb and Parberry using their notation, and the reader is referred to their proofs [5]. Equation (11) can be proved by induction on $b \geq 0$, where $b = 0, 1$ cases are clear from the initial conditions and the recursive relation $U_{a+1}(x) = xU_a(x) + U_{a-1}(x)$. The analog statements concerning $C_n(x)$ and $D_n(x)$ follow easily from Lemma 1. □

Remark: In equations (9)-(10) and (12)-(13), a and b can take any integer value if we define, for all $n \geq 0$, $U_{-n}(x) = (-1)^{n-1}U_n(x)$, $V_{-n}(x) = (-1)^n V_n(x)$, $C_{-n}(x) = -C_n(x)$, and $D_{-n}(x) = D_n(x)$. This definition is also consistent with equations (1), (6), and (7).

Corollary 1: Let p be an odd prime, then

$$V_p(x) \equiv D_p(x) \equiv x^p \pmod{p}. \tag{15}$$

Proof: Consider equation (8). We have

$$\mathrm{E}(p, m) = \frac{4^m}{2^{p-1}} \sum_{j=m}^{\left[\frac{p}{2}\right]} \binom{p}{2j}\binom{j}{m}.$$

Since p is odd we have, for $0 < j \leq \left[\frac{p}{2}\right] < \frac{p}{2}$, the inequality $0 < 2j < p$ and in this range $\binom{p}{2j} \equiv 0$ (mod p). Consequently, $\mathrm{E}(p, m) \equiv 0$ (mod p) if $m > 0$. For $m = 0$, the only nonzero (mod p) term in the sum is the $j = 0$ term. By Fermat's theorem (see [1]), $2^{p-1} \equiv 1$ (mod p) so $\mathrm{E}(p, 0) \equiv 1$ (mod p) and (15) follows. □

Over the field of complex numbers, $U_n(x)$ is a product of $n-1$ distinct linear factors (see [5], Theorem 2):

$$U_n(x) = \prod_{k=1}^{n-1}\left(x - 2i\cos\left(\frac{\pi k}{n}\right)\right), \quad n > 1. \tag{16}$$

This result can be derived from (6) by substituting $x = 2i\cos\theta$ and studying the solutions of $U_n(2i\cos\theta) = 0$. Note that all the nonzero roots are purely imaginary, and since $U_n(x)$ have real coefficients this implies that the nonzero roots come in pairs $(\alpha, -\alpha)$ whose members have equal absolute values and opposite signs. Using (16), Lemma 1, and the last observation, it is also easy to show that

$$C_n(x) = \prod_{k=1}^{n-1}\left(x - 2\cos\left(\frac{\pi k}{n}\right)\right), \quad n > 1.$$

Lemma 2: Let n be a positive integer, $f(x) \in C[x]$, $\theta \in R$. If $2i\cos(n\theta)(2\cos(n\theta))$ is a root of f, then $2i\cos\theta(2\cos\theta)$ is a root of $f(i^{-(n-1)}V_n(x))(f(D_n(x)))$.

Proof: Substituting $x = 2i\cos\theta$ in the expression for $V_n(x)$ in (7), we obtain

$$V_n(2i\cos\theta) = i^n 2\cos(n\theta) = i^{n-1}2i\cos(n\theta).$$

Hence, $f(i^{-(n-1)}V_n(2i\cos\theta)) = f(2i\cos n\theta)$ and the first claim follows. The proof of the second claim is similar. □

Lemma 3: The following expression for the derivative of the n^{th} Fibonacci polynomial holds over any extension field of Z_p for any prime p:

$$(x^2+4)U_n'(x) = nV_n(x) - xU_n(x), \tag{17}$$

and similarly,

$$(x^2-4)C_n'(x) = nD_n(x) - xC_n(x). \tag{18}$$

Proof: First view the Fibonacci polynomials as real valued functions and differentiate using relations (6) and (7) in order to prove the validity of (17) and (18) over the reals. Next, consider the ring homomorphism $Z[x] \to Z_p[x]$, $f(x) \mapsto \bar{f}(x)$, where $\bar{f}(x)$ is the polynomial whose coefficients are the remainders modulo p of the coefficients of $f(x)$. Since both sides of equations (17) and (18) are polynomials over Z [$U_n'(x)$ is the formal algebraic derivative of $U_n(x)$], both equations remain valid when we replace each side with its image under this homomorphism. □

3. FACTORIZATION OF THE FIBONACCI POLYNOMIALS OVER Q

The following definition is inspired by the definition of the cyclotomic polynomials [see equation (2)].

Definition 1: The fibotomic polynomials $P_m(x)$, $Q_{2m}(x)$, $Q_{2m+1}^{\text{odd}}(x)$, and $Q_{2m+1}^{\text{even}}(x)$ are defined by:

$$P_m(x) = \prod_{\substack{k=1 \\ \gcd(k,m)=1}}^{m-1} \left(x - 2i\cos\left(\frac{\pi k}{m}\right)\right), \quad m > 1;$$

$$P_1(x) = 1;$$

$$Q_{2m}(x) = \prod_{\substack{k=1 \\ \gcd(k,2m)=1}}^{2m-1} \left(x - 2\cos\left(\frac{\pi k}{2m}\right)\right), \quad m \geq 1;$$

$$Q_{2m+1}^{\text{odd}}(x) = \prod_{\substack{k=0 \\ \gcd(2k+1,2m+1)=1}}^{m-1} \left(x - 2\cos\left(\frac{(2k+1)\pi}{2m+1}\right)\right), \quad m \geq 1;$$

$$Q_{2m+1}^{\text{even}}(x) = \prod_{\substack{k=1 \\ \gcd(k,2m+1)=1}}^{m} \left(x - 2\cos\left(\frac{2k\pi}{2m+1}\right)\right), \quad m \geq 1;$$

$$Q_1^{\text{even}}(x) = Q_1^{\text{odd}}(x) = 1. \ \square$$

Recall that the set $Z_n^* = \{1 \leq k \leq n-1 \mid \gcd(k,n) = 1\}$, $n \geq 2$, is a group with respect to multiplication modulo n and that $|Z_n^*| = \phi(n)$, where ϕ is the Euler totient function (see [1]). Let

$$(Z_n^*)_{\text{odd}} = \{m \in Z_n^* \mid m \text{ is odd}\} \quad \text{and} \quad (Z_n^*)_{\text{even}} = \{m \in Z_n^* \mid m \text{ is even}\}.$$

Lemma 4: Let $n \neq 3$, $n > 1$, be an integer and let $l \in Z_n^*$ be arbitrary, then Z_n^* is generated by the action of $(Z_n^*)_{\text{odd}}$ on l, i.e., $\forall x \in Z_n^*$, there exist $g_1, \ldots, g_k \in (Z_n^*)_{\text{odd}}$ such that $(g_1 \cdots g_k) \cdot l = x$.

Proof: If n is even, it is obvious that $Z_n^* = (Z_n^*)_{\text{odd}}$ and the claim follows. If n is odd, then $x \mapsto n-x$ is a bijection between the sets $(Z_n^*)_{\text{odd}}$ and $(Z_n^*)_{\text{even}}$; therefore,

$$|(Z_n^*)_{\text{odd}}| = |(Z_n^*)_{\text{even}}| = \frac{1}{2}|Z_n^*| = \frac{1}{2}\phi(n).$$

Now suppose that $(Z_n^*)_{\text{odd}}$ is not a subgroup of Z_n^*. In this case $(Z_n^*)_{\text{odd}}$ generates Z_n^* and therefore the action of $(Z_n^*)_{\text{odd}}$ on any Z_n^* element generates Z_n^*. On the other hand, we will show that the assumption that $(Z_n^*)_{\text{odd}}$ is a subgroup of Z_n^* leads to a contradiction. For any $x \in (Z_n^*)_{\text{even}}$, we have the left coset decomposition $Z_n^* = (Z_n^*)_{\text{odd}} \cup x(Z_n^*)_{\text{odd}}$. Since distinct left cosets are disjoint, this implies $(Z_n^*)_{\text{even}} = x(Z_n^*)_{\text{odd}}$, $\forall x \in (Z_n^*)_{\text{even}}$. Let $n = 2k+1$ with $k \geq 2$. Choose $x = 2 \in (Z_n^*)_{\text{even}}$. By Bertrand's postulate [1], there exists a prime number $k < p < 2k$. The inequality $p > k \geq 2$ implies that p is odd and that $p \nmid 2k+1 = n$ so $p \in (Z_n^*)_{\text{odd}}$. However, since $2k < 2p < 4k$, we have $n < 2p < 2n$. Therefore, $2p = s+n = s$ (mod n); $1 \leq s \leq n-1$, where s is odd. This contradicts $2(Z_n^*)_{\text{odd}} = (Z_n^*)_{\text{even}}$. □

Remark: $(Z_3^*)_{\text{odd}} = \{1\}$ is a proper subgroup of Z_3^*; therefore, the claim of Lemma 4 does not hold in this case.

Lemma 5: The factorization of the Fibonacci polynomials in terms of the fibotomic polynomials is given by

$$U_n(x) = \prod_{d|n} P_d(x), \quad n \geq 1; \tag{19}$$

$$C_{n+1}(x) - C_{n-1}(x) = \prod_{\substack{d|n \\ \frac{n}{d} \text{ is odd}}} Q_{2d}(x), \quad n \geq 1; \tag{20}$$

$$C_{n+1}(x) - C_n(x) = \prod_{2d+1|2n+1} Q_{2d+1}^{\text{odd}}(x), \quad n \geq 0; \tag{21}$$

$$C_{n+1}(x) + C_n(x) = \prod_{2d+1|2n+1} Q_{2d+1}^{\text{even}}(x), \quad n \geq 0. \tag{22}$$

Proof: Equation (19) [which is the analog of (4)] follows from (16) and the definition of $P_d(x)$. To obtain (20)-(22), note that $C_{2n}(x) = C_n(x)(C_{n+1}(x) - C_{n-1}(x))$. [Substitute $a = b = n$ in (14)] and $C_{2n+1}(x) = (C_{n+1}(x) - C_n(x))(C_{n+1}(x) + C_n(x))$ [$a = n+1, b = n$ in (14)]. Using the first relation, we get

$$C_{n+1}(x) - C_{n-1}(x) = \frac{C_{2n}(x)}{C_n(x)} = \prod_{\substack{k=1 \\ k \text{ odd}}}^{2n-1} \left(x - 2\cos\left(\frac{k\pi}{2n}\right)\right).$$

Equation (20) now follows from the definition of $Q_{2d}(x)$. To prove (21)-(22), we need the complex roots of $C_{n+1}(x) \pm C_n(x)$. For example, substituting (6) in $C_{n+1}(x) - C_n(x) = 0$ gives $z^{n+1} - \bar{z}^{n+1} - z^n + \bar{z}^n = 0$, provided that $z \neq \bar{z}$. Since $z\bar{z} = 1$, we get $z^{2n+1} = -1$, which gives

$$C_{n+1}(x) - C_n(x) = \prod_{j=0}^{n-1} \left(x - 2\cos\left(\frac{(2j+1)\pi}{2n+1}\right)\right).$$

Similarly,

$$C_{n+1}(x)+C_n(x)=\prod_{j=1}^{n}\left(x-2\cos\left(\frac{2j\pi}{2n+1}\right)\right).$$

Next, note that the proof of Lemma 4 gives $\deg Q_{2m+1}^{\text{odd}}(x)=\deg Q_{2m+1}^{\text{even}}(x)=\frac{1}{2}\phi(2m+1)$, $m\geq 1$. In order to prove (21), observe that every linear factor,

$$x-2\cos\left(\frac{(2j+1)\pi}{2n+1}\right),$$

of $C_{n+1}(x)-C_n(x)$ divides a $Q_{2d+1}^{\text{odd}}(x)$ on the right-hand side (r.h.s.) of (21), where

$$2d+1=\frac{2n+1}{\gcd(2j+1,2n+1)}.$$

Since all these linear factors are distinct, (21) will follow if both sides have equal degrees. On the left-hand side (l.h.s.) of (21), use $\deg(C_{n+1}(x)-C_n(x))=\deg C_{n+1}(x)=n$. On the r.h.s., use the identity

$$\sum_{\substack{2d+1\mid 2n+1\\ d>0}}\frac{1}{2}\phi(2d+1)=n.$$

Equation (22) may be proved in a similar fashion and will not be presented here. □

Equations (19)-(22) can be inverted with the help of the Möbius function to obtain the analogs of (5) for the fibotomic polynomials. Note that the conditions $d\mid n$, $\frac{n}{d}$ is odd in equation (20) imply that if $n=2^\nu n'$, where n' is an odd integer and ν a nonnegative integer, then $d=2^\nu d'$, where d' is odd and $d'\mid n'$. Hence, we can rewrite (20) as follows:

$$C_{2^\nu n'+1}(x)-C_{2^\nu n'-1}(x)=\prod_{d'\mid n'}Q_{2^{\nu+1}d'}(x).$$

The resulting expressions for the fibotomic polynomials in terms of Fibonacci polynomials are summarized in the following lemma.

Lemma 6:

$$P_n(x)=\prod_{d\mid n}U_d^{\mu(\frac{n}{d})},\quad n\geq 1; \tag{23}$$

$$Q_{2n+1}^{\text{odd}}(x)=\prod_{2d+1\mid 2n+1}(C_{d+1}(x)-C_d(x))^{\mu(\frac{2n+1}{2d+1})},\quad n\geq 1; \tag{24}$$

$$Q_{2m+1}^{\text{even}}(x)=\prod_{2d+1\mid 2n+1}(C_{d+1}(x)+C_d(x))^{\mu(\frac{2n+1}{2d+1})},\quad n\geq 1; \tag{25}$$

$$Q_{2n}(x)=\prod_{d\mid n'}(C_{2^\nu d+1}(x)-C_{2^\nu d-1}(x))^{\mu(\frac{n'}{d})},\quad n\geq 1, \tag{26}$$

where, in (26), $n=2^\nu n'$ and n' is odd. □

Corollary 2: The fibotomic polynomials are monic polynomials with integer coefficients.

Proof: The fact that the fibotomic polynomials are monic is clear from their definition. By (23)-(26), each fibotomic polynomial is a quotient of two monic polynomials over Z whence the claim follows. □

The next lemma lists some more elementary properties of the fibotomic polynomials.

Lemma 7:

(a) $\forall n \geq 3,\ P_n(-x) = P_n(x)$.

(b) $\forall n \geq 1,\ P_{2n}(x) = i^{\phi(2n)} Q_{2n}(-ix)$ and, consequently, $\forall n \geq 2,\ Q_{2n}(-x) = Q_{2n}(x)$.

(c) $\forall n \geq 1,\ Q_{2n+1}^{\text{odd}}(-x) = (-1)^{\frac{1}{2}\phi(2n+1)} Q_{2n+1}^{\text{even}}(x)$.

(d) $\forall n \geq 1,\ P_{2n+1}(x) = (-1)^{\frac{1}{2}\phi(2n+1)} Q_{2n+1}^{\text{odd}}(-ix) Q_{2n+1}^{\text{even}}(-ix)$.

Proof:

(a) By Corollary 2, the coefficients of $P_n(x)$ are real. Applying the remark that follows equation (16), we see that for $n \geq 3$ the roots of $P_n(x)$ also come in pairs of opposite signs; hence, $P_n(x)$ is a product of factors of the form $(x-\alpha)(x+\alpha) = x^2 - \alpha^2$ which are even functions of x.

(b) Compare the definitions of $Q_{2n}(x)$ and $P_{2n}(x)$. Note that $x - \alpha$ is a linear factor of $Q_{2n}(x)$ iff $x - i\alpha$ is a linear factor of $P_{2n}(x)$. The result follows from $x - i\alpha = i(-ix - \alpha)$ and from the fact that $\deg Q_{2n}(x) = \deg P_{2n}(x) = \phi(2n)$.

(c) Using $\deg Q_{2n+1}^{\text{odd}}(x) = \deg Q_{2n+1}^{\text{even}}(x) = \frac{1}{2}\phi(2n+1)$ (see proof of Lemma 5), we get

$$
\begin{aligned}
Q_{2n+1}^{\text{odd}}(-x) &= \prod_{\substack{k=0 \\ \gcd(2k+1,\,2n+1)=1}}^{n-1} \left(-x - 2\cos\left(\frac{(2k+1)\pi}{2n+1}\right)\right) \\
&= (-1)^{\frac{1}{2}\phi(2n+1)} \prod_{\substack{k=0 \\ \gcd(2k+1,\,2n+1)=1}}^{n-1} \left(x + 2\cos\left(\frac{(2k+1)\pi}{2n+1}\right)\right) \\
&= (-1)^{\frac{1}{2}\phi(2n+1)} \prod_{\substack{k=0 \\ \gcd(2k+1,\,2n+1)=1}}^{n-1} \left(x - 2\cos\left(\pi - \frac{(2k+1)\pi}{2n+1}\right)\right) \\
&= (-1)^{\frac{1}{2}\phi(2n+1)} \prod_{\substack{k=0 \\ \gcd(2k+1,\,2n+1)=1}}^{n-1} \left(x - 2\cos\left(\frac{2(n-k)\pi}{2n+1}\right)\right) = (-1)^{\frac{1}{2}\phi(2n+1)} Q_{2n+1}^{\text{even}}(x).
\end{aligned}
$$

(d) Separating the odd and even values of k in the product that defines $P_{2n+1}(x)$, $n \geq 1$, gives

$$
\begin{aligned}
P_{2n+1}(x) &= \prod_{\substack{k=1 \\ \gcd(k,\,2n+1)=1}}^{2n} \left(x - 2i\cos\left(\frac{\pi k}{2n+1}\right)\right) \\
&= \prod_{\substack{k=0 \\ \gcd(2k+1,\,2n+1)=1}}^{n-1} \left(x - 2i\cos\left(\frac{(2k+1)\pi}{2n+1}\right)\right) \prod_{\substack{k=1 \\ \gcd(k,\,2n+1)=1}}^{n} \left(x - 2i\cos\left(\frac{2k\pi}{2n+1}\right)\right) \\
&= \prod_{\substack{k=0 \\ \gcd(2k+1,\,2n+1)=1}}^{n-1} i\left(-ix - 2\cos\left(\frac{(2k+1)\pi}{2n+1}\right)\right) \prod_{\substack{k=1 \\ \gcd(k,\,2n+1)=1}}^{n} i\left(-ix - 2i\cos\left(\frac{2k\pi}{2n+1}\right)\right) \\
&= i^{\phi(2n+1)} Q_{2n+1}^{\text{odd}}(-ix) Q_{2n+1}^{\text{even}}(-ix) = (-1)^{\frac{1}{2}\phi(2n+1)} Q_{2n+1}^{\text{odd}}(-ix) Q_{2n+1}^{\text{even}}(-ix). \quad \square
\end{aligned}
$$

Remark: $(-1)^{\frac{1}{2}\phi(2n+1)} = 1$ if $2n+1$ has two or more distinct prime factors, or is a power of a prime p satisfying $p \equiv 1 \pmod 4$, while otherwise $(-1)^{\frac{1}{2}\phi(2n+1)} = -1$.

4. IRREDUCIBILITY OF THE FIBOTOMIC POLYNOMIALS

In the following, $F_n(x)$ will stand for any of the four fibotomic polynomials $P_{n+1}(x)$, $Q_{2n}(x)$, $Q_{2n+1}^{\text{odd}}(x)$, and $Q_{2n+1}^{\text{even}}(x)$.

Theorem 1: The fibotomic polynomials $F_n(x)$ are irreducible over Q for all $n \geq 1$.

Proof: The irreducibility of $P_2(x) = Q_2(x) = x$, $Q_3^{\text{odd}}(x) = x-1$, and $Q_3^{\text{even}}(x) = x+1$ is clear; hence, we can assume $n \geq 2$. In particular, the roots of the fibotomic polynomials under consideration are nonzero.

Let $f(x)$ be a monic irreducible factor of $F_n(x)$ over Q. We can assume, without loss of generality, that $f(x) \in Z[x]$. The set of complex roots of $f(x)$ must be a subset of R_n, the set of complex roots of $F_n(x)$, and since $\deg f(x) \geq 1$, this subset is not empty. Proving irreducibility of $F_n(x)$ is equivalent to showing that every $\beta \in R_n$ is a root of $f(x)$. Let α denote a given root of $f(x)$, and consider the various polynomials:

1. $F_n(x) = P_{n+1}(x),\ R_n = \left\{\beta_k = 2i\cos\left(\dfrac{\pi k}{n+1}\right) \middle| k \in Z_{n+1}^*\right\},\ \alpha = \beta_l.$

Since $f(x) \in Z[x]$, $-\alpha$ is also a root of $f(x)$. If $n=2$, we get $f(x) = P_3(x)$. To prove the claim of Theorem 1 for $n > 2$, it is sufficient to show that either β_k or $-\beta_k$ is a root of $f(x)$ for all $k \in Z_{n+1}^*$. By Lemma 4, there exists a product j of $(Z_{n+1}^*)_{\text{odd}}$ elements such that $jl \equiv k$ (mod $n+1$) and therefore $2i\cos(\frac{j\cdot l\pi}{n+1}) = \pm\beta_k$. Hence, it is sufficient to show that $2i\cos(\frac{j\cdot l\pi}{n+1})$ is a root of $f(x)$ for any $j \in (Z_{n+1}^*)_{\text{odd}}$. The last statement will follow from the statement that $2i\cos(\frac{p\cdot l\pi}{n+1})$ is a root of $f(x)$ for any odd prime p such that $p \nmid n+1$.

2. $F_n(x) = Q_{2n}(x),\ R_n = \left\{\beta_k = 2\cos\left(\dfrac{\pi k}{2n}\right) \middle| k \in Z_{2n}^*\right\},\ \alpha = \beta_l.$

In this case, $Z_{2n}^* = (Z_{2n}^*)_{\text{odd}}$. For any $k \in (Z_{2n}^*)_{\text{odd}}$, there exists $j \in (Z_{2n}^*)_{\text{odd}}$ such that $l \cdot j = k + s \cdot 2n$ for some integer s. If s is even, $\beta_k = 2\cos(\frac{j\cdot l\pi}{2n})$. If s is odd, then $l\cdot(2n-j) = -k + (l-s)\cdot 2n$, where $l-s$ is even; hence, $\beta_k = 2\cos(\frac{(2n-j)\cdot l\pi}{2n})$. This proves that, for any $k \in (Z_{2n}^*)_{\text{odd}}$, there exists $j \in (Z_{2n}^*)_{\text{odd}}$ such that $2\cos(\frac{k\pi}{2n}) = 2\cos(\frac{j\cdot l\pi}{2n})$. Therefore, it is sufficient to prove that $2\cos(\frac{p\cdot l\pi}{2n})$ is a root of $f(x)$ for any prime p such that $p \nmid 2n$ (in particular, p is odd).

3. $F_n(x) = Q_{2n+1}^{\text{odd}}(x),\ R_n = \left\{\beta_k = 2\cos\left(\dfrac{k\pi}{2n+1}\right) \middle| k \in (Z_{2n+1}^*)_{\text{odd}}\right\},\ \alpha = \beta_l.$

Again, by Lemma 4, for any $k \in (Z_{2n+1}^*)_{\text{odd}}$ there exists a product j of $(Z_{n+1}^*)_{\text{odd}}$ elements such that $l \cdot j = k + s\cdot(2n+1)$ for some integer s. Since l, k, and j are all odd, s must be even, so $\beta_k = 2\cos(\frac{j\cdot l\pi}{2n+1})$. Hence, it will suffice to prove that $2\cos(\frac{p\cdot l\pi}{2n+1})$ is a root of $f(x)$ for any odd prime p such that $p \nmid 2n+1$.

4. $F_n(x) = Q_{2n+1}^{\text{even}}(x)$, $R_n = \left\{\beta_k = 2\cos\left(\dfrac{k\pi}{2n+1}\right) \middle| k \in (Z_{2n+1}^*)_{\text{even}}\right\}$, $\alpha = \beta_l$.

Due to Lemma 4, for any $k \in (Z_{2n+1}^*)_{\text{even}}$, there exists a product j of $(Z_{n+1}^*)_{\text{odd}}$ elements such that $l \cdot j = k + s \cdot (2n+1)$ for some integer s. Since l and k are even, s must be even, resulting in $\beta_k = 2\cos\left(\frac{j \cdot l\pi}{2n+1}\right)$. Hence, it will suffice to prove that $2\cos\left(\frac{p \cdot l\pi}{2n+1}\right)$ is a root of $f(x)$ for any odd prime p such that $p \nmid 2n+1$.

Suppose then that $2\varepsilon_F \cos(\theta_F)$ is a root of $f(x)$, where ε_F and θ_F depend on the particular $F_n(x)$ under consideration [e.g., if $F_n(x) = P_{n+1}(x)$, $\varepsilon_F = i$, and $\theta_F = \frac{l\pi}{n+1}$] and that, contrary to what we want to prove, there exists some odd prime p not dividing the denominator of θ_F such that $2\varepsilon_F \cos(p \cdot \theta_F)$ is not a root of $f(x)$. Hence, there exists a polynomial $g(x) \in Z[x]$ such that $F_n(x) = f(x)g(x)$ and $2\varepsilon_F \cos(p \cdot \theta_F)$ is a root of $g(x)$. By Lemma 2, $2\varepsilon_F \cos(\theta_F)$ is a root of $g(i^{-(p-1)}V_p(x))$ if $F_n(x) = P_{n+1}(x)$ and a root of $g(D_p(x))$ in the other cases. Therefore, $\gcd(f(x), g(i^{-(p-1)}V_p(x))) \neq 1$ if $F_n(x) = P_{n+1}(x)$ and $\gcd(f(x), g(D_p(x))) \neq 1$ in the other cases. Under $Z[x] \to Z_p[x]$, $f(x) \mapsto \bar{f}(x)$ (see proof of Lemma 3), we have $\gcd(f(x), g(i^{-(p-1)}V_p(x))) \mapsto \gcd(\bar{f}(x), \bar{g}(i^{-(p-1)}\bar{V}_p(x)))$ and $\gcd(f(x), g(D_p(x))) \mapsto \gcd(\bar{f}(x), \bar{g}(\bar{D}_p(x)))$. As $\gcd(f(x), g(i^{-(p-1)}V_p(x)))$ and $\gcd(f(x), g(D_p(x)))$ are nonscalar monic polynomials, so are $\gcd(\bar{f}(x), \bar{g}(i^{-(p-1)}\bar{V}_p(x)))$ and $\gcd(\bar{f}(x), \bar{g}(\bar{D}_p(x)))$. Using Corollary 1, $V_p(x) \equiv D_p(x) \equiv x^p \pmod p$ so that $\bar{g}(i^{-(p-1)}\bar{V}_p(x)) \equiv \bar{g}(\bar{D}_p(x)) \equiv \bar{g}(x^p) \pmod p$. Note that the congruence

$$\bar{g}(i^{-(p-1)}\bar{V}_p(x)) \equiv \bar{g}\left((-1)^{-\left(\frac{p-1}{2}\right)} x^p\right) \equiv \bar{g}(x^p) \pmod p$$

in the case $F_n(x) = P_{n+1}(x)$ is justified by the fact that g, and therefore $\bar{g}$, is an even polynomial. g is even since $g \in Z[x]$, its roots are also roots of $U_{n+1}(x)$, and therefore the argument used in the proof of the first claim of Lemma 7 applies. We conclude that $\deg(\gcd(\bar{f}(x), \bar{g}(x^p))) > 0$; thus, due to Frobenius' field automorphism, $Z_p[x] \to Z_p[x]$, $x \mapsto x^p$, $\deg(\gcd(\bar{f}(x), (\bar{g}(x))^p)) > 0$, and hence $\deg(\gcd(\bar{f}(x), \bar{g}(x))) > 0$. Consequently, $\bar{f}(x)\bar{g}(x)$ has a multiple root in some extension field of $Z_p[x]$ [note that $\deg d > 0$, where $d = \gcd(\bar{f}(x)\bar{g}(x))$, remains true in any extension field and that $d^2 \mid \bar{f}(x)\bar{g}(x)$]. This implies that $\bar{F}_n(x)$ has a multiple root in some extension field of $Z_p[x]$. However, since $F_n(x)$ divides some Fibonacci polynomial, this implies there is a prime $p \geq 3$ and an integer $m \geq 4$ such that $p \nmid m$ and $\bar{U}_m(x)$ or $\bar{C}_m(x)$ has a multiple root in some extension field of $Z_p[x]$. By proving the impossibility of this last statement, we will obtain the desired contradiction.

Any multiple root of $\bar{U}_m(x)(\bar{C}_m(x))$ is also a root of the formal derivative $\bar{U}_m'(x)(\bar{C}_m'(x))$. For $p \geq 3$, $p \nmid m$, we have $\overline{m}\bar{V}_m(x) \neq 0$ and $\overline{m}\bar{D}_m(x) \neq 0$. Hence, by equations (17)-(18), a multiple root of $\bar{U}_m(x)(\bar{C}_m(x))$ is also a root of $\bar{V}_m(x)(\bar{D}_m(x))$. Now, taking $a = m$ and $b = m-1$ in (9)-(10) and in (12)-(13), and taking the difference of the two equations in each pair, we get

$$U_{m-1}(x)V_m(x) - U_m(x)V_{m-1}(x) = 2(-1)^m \quad \text{and} \quad C_{m-1}(x)D_m(x) - C_m(x)D_{m-1}(x) = -2.$$

Since the characteristic of the fields of interest is different from 2, the preceding two equations imply

$$\gcd(\overline{U}_m(x), \overline{V}_m(x)) = 1 \quad \text{and} \quad \gcd(\overline{C}_m(x), \overline{D}_m(x)) = 1;$$

thus, $\overline{U}_m(x)$ and $\overline{V}_m(x)$ do not have a common root, nor do $\overline{C}_m(x)$ and $\overline{D}_m(x)$. □

Theorem 1 can be generalized to the field $Q[i]$ in the following way.

Theorem 2: The fibotomic polynomials $P_{2n}(x)$, $Q_{2n}(x)$, $Q_{2n+1}^{\text{odd}}(x)$, $Q_{2n+1}^{\text{even}}(x)$ are irreducible over $Q[i]$ for all $n \geq 1$.

Proof: It is not hard to see that the proof of Theorem 1 is applicable in this case, with minor modifications, for $Q[i]$. The main point that requires attention is the claim that, if $f(x)$ is a factor of $P_m(x)$ and β is a root of $f(x)$, then $-\beta$ is also a root of $f(x)$. This claim is not valid anymore as it was based on the assumption that the coefficients of $f(x)$ are real. If we look closely at the use of this claim in the proof, we see that it is needed only for odd m values. For even m values, we can show that, if

$$\alpha = 2i\cos\left(\frac{l\pi}{m}\right),$$

where $l \in Z_m^*$ is some fixed value, then for any $k \in Z_m^*$ there exists $j \in (Z_m^*)_{\text{odd}}$ such that

$$\beta = 2i\cos\left(\frac{k\pi}{m}\right) = 2i\cos\left(\frac{j \cdot l\pi}{m}\right)$$

by the same argument that was used in the $Q_{2m}(x)$ case. In fact, $P_{2n+1}(x)$ is reducible over $Q[i]$ for all $n \geq 1$, as is evident from claim (d) of Lemma 7, which gives its prime factorization over $Q[i]$. □

5. CONCLUDING REMARKS

Formulas (19)-(22) give the prime factorization of $U_n(x)$ and $C_n(x)$ over Q. The prime factorization of $V_n(x)$ and $D_n(x)$ over Q can be deduced from the prime factorization of $U_n(x)$ and $C_n(x)$ over Q with the help of equations (10) and (12). Taking $a = b = n$ in these equations gives

$$V_n(x) = \frac{U_{2n}(x)}{U_n(x)} \quad \text{and} \quad D_n(x) = \frac{C_{2n}(x)}{C_n(x)},$$

and the r.h.s. of the last two relations can be expressed as products of fibotomic polynomials.

Returning to the more general solutions of (1), we find that the Q-irreducible factorization of the one-variable polynomials $F_n(x, b)$ and $L_n(x, b)$, where b is some fixed nonzero integer, can be obtained from our previous results. This follows from the observation that if $b > 0$, then

$$F_n(x, b) = (\sqrt{b})^{n-1} U_n\left(\frac{x}{\sqrt{b}}\right) \quad \text{and} \quad L_n(x, b) = (\sqrt{b})^n V_n\left(\frac{x}{\sqrt{b}}\right),$$

while if $b < 0$, then

$$F_n(x, b) = (\sqrt{-b})^{n-1} C_n\left(\frac{x}{\sqrt{-b}}\right) \quad \text{and} \quad L_n(x, b) = (\sqrt{-b})^n D_n\left(\frac{x}{\sqrt{-b}}\right).$$

For instance, note that if n is odd then $(\sqrt{b})^{n-1}$ is an integer and all irreducible factors of $U_n(x)$ are in fact polynomials in x^2 [see Lemma 7(a)]. Hence, using equation (19) for the r.h.s. of

$$F_n(x, b) = (\sqrt{b})^{n-1} U_n\left(\frac{x}{\sqrt{b}}\right)$$

gives the irreducible factorization of the l.h.s. over Q. If n is even, we first "pull out" a factor $\frac{x}{\sqrt{b}}$ from $U_n(\frac{x}{\sqrt{b}})$ and then apply a similar argument.

Finally, I would like to point out a relation between the present work and certain formulas used in the work of Brillhart, Montgomery, and Silverman [2] for the preparation of factorization tables of Fibonacci and Lucas numbers. These authors use the two-variable homogenous cyclotomic polynomials

$$\Phi_d(x', y') = y'^{\phi(d)}\Phi_d\left(\frac{x'}{y'}\right)$$

[see equations (2)-(4)] in order to express the Fibonacci numbers as products of "primitive parts." This is done in the following way. Using (4), we have

$$x'^n - y'^n = \prod_{d\mid n}\Phi_d(x', y').$$

Substituting $x' = w$, $y' = \overline{w}$ (see Proposition 1) and using equation (6), we get

$$(w-\overline{w})U_n(x) = w^n - \overline{w}^n = \prod_{d\mid n}\Phi_d(w, \overline{w}).$$

By Möbius inversion, one gets

$$\phi_d(w, \overline{w}) = \prod_{\delta\mid d} U_\delta^{\mu(d/\delta)}(x).$$

The reason that the factor $(w-\overline{w})$ which multiplied $U_n(x)$ "disappeared" from the r.h.s. is that two possible nonzero values of the Möbius function, ±1, occur an equal number of times in the product. In the terminology of [2], $\Phi_d(w, \overline{w})$, $d \geq 2$, is called the primitive part of $U_d(x)$. (Strictly speaking, [2] focuses only on the case $x = 1$.) Comparing with equation (23), we obtain the following direct relation between the cyclotomic and fibotomic polynomials:

$$P_n(x) = \Phi_n(w, \overline{w}),\ n \geq 2.$$

ACKNOWLEDGMENTS

I wish to thank Ido Efrat for a helpful conversation and the anonymous referee for useful remarks.

REFERENCES

1. J. A. Anderson & J. M. Bell. *Number Theory with Applications*. Prentice Hall, 1996.
2. J. Brillhart, P. L. Montgomery, & R. D. Silverman. "Tables of Fibonacci and Lucas Factorizations." *Math. Comp.* **50.141** (1988):251.
3. B. Conolly & S. Vajda. *A Mathematical Kaleidoscope*. Albion Publishing Press, 1995.
4. S. Lang. *Algebra*. 3rd ed. New York: Addison-Wesley, 1993.
5. W. Webb & E. Parberry. "Divisibility Properties of Fibonacci Polynomials." *The Fibonacci Quarterly* **7.5** (1969):457.

AMS Classification Numbers: 11B39