CHARACTERIZATION OF THE STRONG DIVISIBILITY PROPERTY FOR GENERALIZED FIBONACCI POLYNOMIALS

Rigoberto Flórez[1]
Department of Mathematics and Computer Science, The Citadel, Charleston, South Carolina
rigo.florez@citadel.edu

Robinson A. Higuita
Instituto de Matemáticas, Universidad de Antioquia, Medellín, Colombia
robinson.higuita@udea.edu.co

Antara Mukherjee[2]
Department of Mathematics and Computer Science, The Citadel, Charleston, South Carolina
antara.mukherjee@citadel.edu

Received: 11/18/16, Revised: 9/14/17, Accepted: 2/20/18, Published: 3/9/18

Abstract

It is known that the greatest common divisor of two Fibonacci numbers is again a Fibonacci number. This is called the *strong divisibility property*. However, strong divisibility does not hold for every second order sequence. In this paper we study the generalized Fibonacci polynomials and classify them in two types depending on their Binet formula. We give a complete characterization of those polynomials that satisfy the strong divisibility property. We also give formulas to calculate the greatest common divisor of those polynomials that do not satisfy the strong divisibility property.

1. Introduction

It is well-known that the greatest common divisor (gcd) of two Fibonacci numbers is a Fibonacci number [19]. In fact, $\gcd(F_m, F_n) = F_{\gcd(m,n)}$. This is called the *strong divisibility property* or *Fibonacci gcd property*. We study divisibility properties of generalized Fibonacci polynomials (GFP) and in particular we give a characterization of the strong divisibility property for these polynomials.

[1]Partially supported by The Citadel Foundation.
[2]Partially supported by The Citadel Foundation.

We classify the GFPs into two types, the Lucas type and the Fibonacci type, depending on their closed formulas or their Binet formulas (see for example, $L_n(x)$ (4) and $R_n(x)$ (6), and Table 2). That is, if after solving the characteristic polynomial of a GFP sequence we obtain a closed formula that looks like the Binet formula for Fibonacci (Lucas) numbers, we call the sequence a Fibonacci (Lucas) type sequence. Familiar examples of Fibonacci type polynomials are: Fibonacci polynomials, Pell polynomials, Fermat polynomials, Chebyshev polynomials of the second kind, Jacobsthal polynomials, and one type of Morgan-Voyce polynomials. Examples of Lucas type polynomials are: Lucas polynomials, Pell-Lucas polynomials, Fermat-Lucas polynomials, Chebyshev polynomials of the first kind, Jacobsthal-Lucas polynomials, and the second type of Morgan-Voyce polynomials. Horadam [13] and André-Jeannin [1] have studied these polynomials in detail.

In Theorem 3 we prove that a GFP satisfies the strong divisibility property if and only if it is of Fibonacci type. Theorem 1 shows that the Lucas type polynomials partially satisfy the strong divisibility property and also gives the gcd for those cases in which the property is not satisfied.

A Lucas type polynomial is equivalent (or conjugate) to a Fibonacci type polynomial if they both have the same recurrence relation but different initial conditions (see also Flórez et al. [4]). Theorem 2 proves that two equivalent GFPs partially satisfy the strong divisibility property and gives the gcd for those cases in which the property is not satisfied.

In 1969 Webb and Parberry [26] extended the strong divisibility property to Fibonacci polynomials. In 1974 Hoggatt and Long [12] proved the strong divisibility property for one type of generalized Fibonacci polynomial. In 1978 Hoggatt and Bicknell-Johnson [11] extended the result mentioned in [12] to some cases of Fibonacci type polynomials. In 2005 Rayes, et al. [24] proved that the strong divisibility property holds partially for the Chebyshev polynomials (we prove the general result in Theorem 1). Over the years several other authors [2, 3, 8, 16, 17, 18, 20, 21, 22, 23, 25] have also been interested in the divisibility properties of sequences.

Lucas [20] proved the strong divisibility property (SDP) for Fibonacci numbers. However, the study of the SDP for Lucas numbers did not occur until 1991, when McDaniel [21] proved that the Lucas numbers partially satisfy the SDP. In 1995 Hilton, et al. [10] gave some more precise results about this property. As mentioned above, several authors have been interested in the divisibility properties for Fibonacci type polynomials. However, the Lucas type polynomials have been less studied. Here we give a complete study of all three cases of the SDP. Indeed, we give a characterization of the SDP for Fibonacci type polynomials and study both the SDP for Lucas type polynomials and the SDP for the combinations of Lucas type polynomials and Fibonacci type polynomials. Finally we provide an open question for the most general case of the combination of two polynomials.

2. Generalized Fibonacci Polynomials

In the literature there are several definitions of generalized Fibonacci polynomials. The definition that we introduce here is simpler and covers other definitions. The background given in this section is a summary of the background given in [4]. However, the definition of generalized Fibonacci polynomial here is not exactly the same as in [4]. The *generalized Fibonacci polynomial* sequence $\{G_n(x)\}$, denoted by GFP, is defined by the following recurrence relation: if $p_0(x)$ is a constant and $p_1(x)$, $d(x)$, and $g(x)$ are non-zero polynomials in $\mathbb{Z}[x]$ with $\gcd(d(x), g(x)) = 1$, then

$$G_0(x) = p_0(x),\ G_1(x) = p_1(x), \text{ and } G_n(x) = d(x)G_{n-1}(x) + g(x)G_{n-2}(x) \qquad (1)$$

for $n \geq 2$.

For example, if we let $p_0(x) = 0$, $p_1(x) = 1$, $d(x) = x$, and $g(x) = 1$ we obtain the regular Fibonacci polynomial sequence. Thus,

$$F_0(x) = 0,\ F_1(x) = 1, \text{ and } F_n(x) = xF_{n-1}(x) + F_{n-2}(x) \text{ for } n \geq 2.$$

Letting $x = 1$ and choosing the correct values for $p_0(x)$, $p_1(x)$, $d(x)$, and $g(x)$, the generalized Fibonacci polynomial sequence gives rise to three classical numerical sequences: the Fibonacci sequence, the Lucas sequence and the generalized Fibonacci sequence.

Table 1 provides familiar examples of the GFPs (see [4, 14, 15, 19]). Schechter polynomials [11] are also examples of generalized Fibonacci polynomials.

Polynomial	Initial value $G_0(x) = p_0(x)$	Initial value $G_1(x) = p_1(x)$	Recursive Formula $G_n(x) = d(x)G_{n-1}(x) + g(x)G_{n-2}(x)$
Fibonacci	0	1	$F_n(x) = xF_{n-1}(x) + F_{n-2}(x)$
Lucas	2	x	$D_n(x) = xD_{n-1}(x) + D_{n-2}(x)$
Pell	0	1	$P_n(x) = 2xP_{n-1}(x) + P_{n-2}(x)$
Pell-Lucas	2	$2x$	$Q_n(x) = 2xQ_{n-1}(x) + Q_{n-2}(x)$
Pell-Lucas-prime	1	x	$Q_n^{'}(x) = 2xQ_{n-1}^{'}(x) + Q_{n-2}^{'}(x)$
Fermat	0	1	$\Phi_n(x) = 3x\Phi_{n-1}(x) - 2\Phi_{n-2}(x)$
Fermat-Lucas	2	$3x$	$\vartheta_n(x) = 3x\vartheta_{n-1}(x) - 2\vartheta_{n-2}(x)$
Chebyshev second kind	0	1	$U_n(x) = 2xU_{n-1}(x) - U_{n-2}(x)$
Chebyshev the first kind	1	x	$T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x)$
Jacobsthal	0	1	$J_n(x) = J_{n-1}(x) + 2xJ_{n-2}(x)$
Jacobsthal-Lucas	2	1	$j_n(x) = j_{n-1}(x) + 2xj_{n-2}(x)$
Morgan-Voyce	0	1	$B_n(x) = (x+2)B_{n-1}(x) - B_{n-2}(x)$
Morgan-Voyce	2	$x+2$	$C_n(x) = (x+2)C_{n-1}(x) - C_{n-2}(x)$
Vieta	0	1	$V_n(x) = xV_{n-1}(x) - V_{n-2}(x)$
Vieta-Lucas	2	x	$v_n(x) = xv_{n-1}(x) - v_{n-2}(x)$

Table 1: Recurrence relation of some GFPs.

2.1. Fibonacci Type and Lucas Type Polynomials

If we impose some conditions on Definition (1) we obtain two types of distinguishable polynomials. We say that a sequence as in (1) is Lucas type or the first type, if $2p_1(x) = p_0(x)d(x)$ with $p_0 \neq 0$. We say that a sequences as in (1) is Fibonacci type or the second type if $p_0(x) = 0$ and $p_1(x)$ a non-zero constant.

If $d^2(x) + 4g(x) > 0$, then the explicit formula for the recurrence relation (1) is given by

$$G_n(x) = t_1 a^n(x) + t_2 b^n(x) \tag{2}$$

where $a(x)$ and $b(x)$ are the solutions of the quadratic equation associated with the second order recurrence relation $G_n(x)$. That is, $a(x)$ and $b(x)$ are the solutions of $z^2 - d(x)z - g(x) = 0$. The explicit formula for $G_n(x)$ given in (2) with $G_0(x) = p_0(x)$ and $G_1(x) = p_1(x)$ implies that

$$t_1 = \frac{p_1(x) - p_0(x)b(x)}{a(x) - b(x)} \quad \text{and} \quad t_2 = \frac{-p_1(x) + p_0(x)a(x)}{a(x) - b(x)}. \tag{3}$$

Using (2) and (3) we obtain the Binet formulas for the generalized Fibonacci sequences of Lucas type and Fibonacci type. Thus, substituting $2p_1(x) = p_0(x)d(x)$ in (3) we obtain that $t_1 = t_2 = p_0(x)/2$. Substituting these values of t_1 and t_2 in (2) and letting α be $2/p_0(x)$ we obtain: the Binet formula for generalized Fibonacci sequence of Lucas type,

$$L_n(x) = \frac{a^n(x) + b^n(x)}{\alpha}. \tag{4}$$

We want α to be an integer, and therefore $|p_0(x)| = 1$ or 2.

Now, substituting $p_0(x) = 0$ and the constant $p_1(x)$ in (3) we obtain that $t_1 = t_2 = p_1(x)$. Substituting this in (2) we obtain the Binet formula for the generalized Fibonacci sequence of Fibonacci type,

$$R_n(x) = \frac{p_1(x)\left(a^n(x) - b^n(x)\right)}{a(x) - b(x)}. \tag{5}$$

In this paper we are interested only in $R_n(x)$ when $p_1(x) = 1$ (see also [12]). Therefore, the Binet formula $R_n(x)$ used here is:

$$R_n(x) = \frac{a^n(x) - b^n(x)}{a(x) - b(x)}. \tag{6}$$

Note that if $d(x)$ and $g(x)$ are the polynomials defined in (1), then $a(x)+b(x) = d(x)$, $a(x)b(x) = -g(x)$, and $a(x) - b(x) = \sqrt{d^2(x) + 4g(x)}$.

The sequence of polynomials that have Binet representations $R_n(x)$ or $L_n(x)$ depend only on $d(x)$ and $g(x)$ defined in (1). We say that a generalized Fibonacci sequence of Lucas (Fibonacci) type is *equivalent*, or the *conjugate*, to a sequence of the Fibonacci (Lucas) type, if their recursive sequences are determined by the same polynomials $d(x)$ and $g(x)$. Notice that two equivalent polynomials have the same $a(x)$ and $b(x)$ in their Binet representations.

For example, the Lucas polynomial is a GFP of Lucas type, whereas the Fibonacci polynomial is a GFP of Fibonacci type. Lucas and Fibonacci polynomials are equivalent because $d(x) = x$ and $g(x) = 1$ for both (see Table 1). Note that in their Binet representations they both have $a(x) = (x + \sqrt{x^2+4})/2$ and $b(x) = (x - \sqrt{x^2+4})/2$. Table 2 is based on information from the following papers [1, 4, 13]. The leftmost polynomials in Table 2 are of the Lucas type and their equivalent polynomials are in the second column on the same line. In the last two columns of Table 2 are the $a(x)$ and $b(x)$ that the pairs of equivalent polynomials share. It is easy to obtain the characteristic equations of the sequences given in Table 1 where the roots of each equation are given by $a(x)$ and $b(x)$.

For the sake of simplicity throughout this paper we use a in place of $a(x)$ and b in place of $b(x)$ when they appear in the Binet formulas. We use the notation G_n^* or G_n' for G_n depending on whether it satisfies the Binet formulas (4) or (6), respectively, (see Section 4).

For most of the proofs of GFPs of Lucas type it is required that

$$\gcd(p_0(x), p_1(x)) = 1, \quad \gcd(p_0(x), d(x)) = 1, \quad \text{and} \quad \gcd(d(x), g(x)) = 1.$$

It is easy to see that $\gcd(\alpha, G_n^*(x)) = 1$. Therefore, for the rest of the paper we suppose that these conditions mentioned hold for all GFP sequences of Lucas type treated here. We use ρ to denote $\gcd(d(x), G_1(x))$. Notice that in the definition of Pell-Lucas we have $p_0(x) = 2$ and $p_1(x) = 2x$. Thus, the $\gcd(p_0(x), p_1(x)) \neq 1$. Therefore, Pell-Lucas does not satisfy the extra conditions that were just imposed on the GFPs. To solve this problem we define *Pell-Lucas-prime* as follows:

$$Q_0^{'}(x) = 1,\ Q_1^{'}(x) = x,\ \text{and}\ Q_n^{'}(x) = 2xQ_{n-1}^{'}(x) + Q_{n-2}^{'}(x) \text{ for } n \geq 2.$$

It easy to see that $2Q_n^{'}(x) = Q_n(x)$ and that $\alpha = 2$. Flórez, et al. [5] worked on similar problems for numerical sequences.

Note. The definition of GFPs in [4] differs from the definition in this paper due to the initial conditions of the Fibonacci type polynomials. Thus, the initial condition for the Fibonacci type polynomials in [4] is $G_0(x) = p_0(x) = 1$ and so implicitly $G_{-1}(x) = 0$. However, our definition for the Lucas type polynomials is the same in both papers.

3. Divisibility Properties of GFPs

In this section we prove a few divisibility and gcd properties which are true for all GFPs. These results will be used in a later section to prove the main results of this paper.

Polynomial Lucas type	Polynomial of Fibonacci type	$a(x)$	$b(x)$
Lucas	Fibonacci	$(x+\sqrt{x^2+4})/2$	$(x-\sqrt{x^2+4})/2$
Pell-Lucas-prime	Pell	$x+\sqrt{x^2+1}$	$x-\sqrt{x^2+1}$
Fermat-Lucas	Fermat	$(3x+\sqrt{9x^2-8})/2$	$(3x-\sqrt{9x^2-8})/2$
Chebyshev 1st kind	Chebyshev 2nd kind	$x+\sqrt{x^2-1}$	$x-\sqrt{x^2-1}$
Jacobsthal-Lucas	Jacobsthal	$(1+\sqrt{1+8x})/2$	$(1-\sqrt{1+8x})/2$
Morgan-Voyce	Morgan-Voyce	$(x+2+\sqrt{x^2+4x})/2$	$(x+2-\sqrt{x^2+4x})/2$
Vieta-Lucas	Vieta	$(x+\sqrt{x^2-4})/2$	$(x-\sqrt{x^2-4})/2$

Table 2: $R_n(x)$ equivalent to $L_n(x)$.

Proposition 1 parts (1) and (2) is a generalization of Proposition 2.2 in [6]. The proof here is similar to the proof in [6] since both use properties of integral domains. The reader can therefore update the proof in the afore-mentioned paper to obtain the proof of this proposition.

Proposition 1. *Let $p(x), q(x), r(x)$, and $s(x)$ be polynomials.*

(1) If $\gcd(p(x), q(x)) = \gcd(r(x), s(x)) = 1$, then $\gcd(p(x)q(x), r(x)s(x))$ is equal to $\gcd(p(x), r(x)) \gcd(p(x), s(x)) \gcd(q(x), r(x)) \gcd(q(x), s(x))$.

(2) If $\gcd(p(x), r(x)) = 1$ and $\gcd(q(x), s(x)) = 1$, then

$$\gcd(p(x)q(x), r(x)s(x)) = \gcd(p(x), s(x)) \gcd(q(x), r(x)).$$

(3) If $z_1(x) = \gcd(p(x), r(x))$ and $z_2(x) = \gcd(q(x), s(x))$, then

$$\gcd(p(x)q(x), r(x)s(x)) = \frac{\gcd(z_2(x)p(x), z_1(x)s(x)) \gcd(z_1(x)q(x), z_2(x)r(x))}{z_1(x)z_2(x)}.$$

Proof. We prove part (3). Since $\gcd(p(x), r(x)) = z_1(x)$ and $\gcd(q(x), s(x)) = z_2(x)$, there are polynomials $P(x)$, $S(x)$, $Q(x)$, and $R(x)$ with

$$\gcd(P(x), R(x)) = \gcd(Q(x), S(x)) = 1,$$

such that $p(x) = z_1(x)P(x)$, $s(x) = z_2(x)S(x)$, $r(x) = z_1(x)R(x)$, and $q(x) = z_2(x)Q(x)$. So,

$$\begin{aligned} \gcd(p(x)q(x), r(x)s(x)) &= \gcd(z_1(x)P(x)z_2(x)Q(x), z_1(x)R(x)z_2(x)S(x)) \\ &= z_1(x)z_2(x) \gcd(P(x)Q(x), R(x)S(x)). \end{aligned}$$

From part (2) we know that

$$\gcd(P(x)Q(x), R(x)S(x)) = \gcd(P(x), S(x)) \gcd(Q(x), R(x)).$$

Now it is easy to see that

$$\gcd(p(x)q(x), r(x)s(x)) = \frac{\gcd(z_2(x)p(x), z_1(x)s(x))\gcd(z_1(x)q(x), z_2(x)r(x))}{z_1(x)z_2(x)}.$$

This proves part (3). □

We recall that $\rho = \gcd(d(x), G_1(x))$ and that for GFPs of Lucas type it is required that $\gcd(p_0(x), p_1(x)) = 1$, $\gcd(p_0(x), d(x)) = 1$, $\gcd(p_0(x), g(x)) = 1$, and that $\gcd(d(x), g(x)) = 1$. We also recall that $p_0(x) = 0$ and $p_1(x) = 1$ for GFPs of Fibonacci type.

For the rest of the paper we use the notation G_n^* if the GFP G_n satisfies the Binet formula (4) and G_n' if the GFPs G_n satisfies the Binet formula (6). We use G_n if the result does not need the mentioned classification to be true. We recall that for Lucas type polynomials $|p_0(x)| = 1$ or 2 and for Fibonacci type polynomials $p_1(x) = 1$. Lemma 1 part (3) is [12, Lemma 3].

Lemma 1. *If $G_n(x)$ is a GFP of either Lucas or Fibonacci type, then*

(1) $\gcd(d(x), G_{2n+1}(x)) = G_1(x)$ *for every positive integer n.*

(2) If the GFP is of Lucas type, then $\gcd(d(x), G_{2n}^*(x)) = 1$ *and if the GFP is of Fibonacci type, then* $\gcd(d(x), G_{2n}'(x)) = d(x)$.

(3) If n is a positive integer, then $\gcd(g(x), G_n(x)) = \gcd(g(x), G_1(x)) = 1$.

Proof. We prove part (1) by induction. Let G_n be a GFP and let $S(n)$ be the statement

$$\rho = \gcd(d(x), G_{2n+1}(x)) \text{ for } n \geq 1.$$

To prove $S(1)$ we suppose that $\gcd(d(x), G_3(x)) = r$. Thus, r divides any linear combination of $d(x)$ and $G_3(x)$. Therefore, r divides $G_3(x) - d(x)G_2(x)$. This and given that $G_3(x) = d(x)G_2(x) + g(x)G_1(x)$ imply that $r \mid g(x)G_1(x)$. So, $r \mid \gcd(d(x), g(x)G_1(x))$. Since $\gcd(d(x), g(x)) = 1$, we have $r \mid \rho$. It is easy to see that $\rho \mid r$. Thus, $r = \gcd(d(x), G_1(x))$. This proves $S(1)$.

We suppose that $S(n)$ is true for $n = k - 1$. That is, $\gcd(d(x), G_{2k-1}(x)) = \rho$. To prove $S(k)$ we suppose that $\gcd(d(x), G_{2k+1}(x)) = r'$. Thus, r' divides any linear combination of $d(x)$ and $G_{2k+1}(x)$. Therefore, $r' \mid (G_{2k+1}(x) - d(x)G_{2k}(x))$. This and $G_{2k+1}(x) = d(x)G_{2k}(x) + g(x)G_{2k-1}(x)$ imply that $r' \mid g(x)G_{2k-1}(x)$. Therefore, $r' \mid \gcd(d(x), g(x)G_{2k-1}(x))$. Since $\gcd(d(x), g(x)) = 1$, we have that r' divides the $\gcd(d(x), G_{2k-1}(x))$. By the inductive hypothesis we know that $\gcd(d(x), G_{2k-1}(x)) = \rho$. Thus, $r' \mid \rho$. It is easy to see that $\gcd(d(x), G_{2k+1}(x))$ divides r'. So, $r' = \gcd(G_1(x), d(x))$.

We show that depending on the type of sequence, it holds that $\gcd(d(x), G_1(x))$ is equal to G_1. If $G_n(x)$ is a GFP of Fibonacci type, then by definition of $p(x)$ we have $G_1(x) = 1$ (see comments after Binet formula (5)). Suppose that $G_n(x)$ is a GFP of Lucas type. Recall that $2p_1(x) = p_0(x)d(x)$ and that $|p_0(x)| = 1$ or 2. The conclusion is straightforward since $G_1(x) = (a(x) + b(x))/\alpha = d(x)/\alpha$.

Proof of part (2). Let $S(n)$ be the statement

$$\rho = \gcd(d(x), G_{2n}(x)) \text{ for } n \geq 1.$$

To prove $S(2)$ we suppose that $\gcd(d(x), G_4(x)) = r$. Thus, r divides any linear combination of $d(x)$ and $G_4(x)$. Therefore, r divides $G_4(x) - d(x)G_3(x)$. This, and given that $G_4(x) = d(x)G_3(x) + g(x)G_2(x)$, imply that $r \mid g(x)G_2(x)$. Therefore, $r \mid \gcd(d(x), g(x)G_2(x))$. Since $\gcd(d(x), g(x)) = 1$, we have $r \mid \rho$. It is easy to see that $\rho \mid r$. Thus, $r = \gcd(d(x), G_2(x))$. This proves $S(2)$.

We suppose that $S(n)$ is true for $n = k - 1$. That is, $\gcd(d(x), G_{2k-2}(x)) = \rho$. To prove $S(k)$ we suppose that $\gcd(d(x), G_{2k}(x)) = r'$. Thus, r' divides any linear combination of $d(x)$ and $G_{2k}(x)$. So, $r' \mid (G_{2k}(x) - d(x)G_{2k-1}(x))$. This and $G_{2k}(x) = d(x)G_{2k-1}(x) + g(x)G_{2k-2}(x)$ imply that $r' \mid g(x)G_{2k-2}(x)$. Therefore, $r' \mid \gcd(d(x), g(x)G_{2k-2}(x))$. Since $\gcd(d(x), g(x)) = 1$, we have that r' divides the $\gcd(d(x), G_{2k-2}(x))$. From the inductive hypothesis we know that $\gcd(d(x), G_{2k-2}(x)) = \rho$. Thus, $r' \mid \rho$. It is easy to see that $\gcd(d(x), G_{2k}(x))$ divides r'. Therefore, $r' = \gcd(G_2(x), d(x))$.

We observe that for a GFP of Fibonacci type it holds that $G'_2(x) = a(x)+b(x) = d(x)$. So, it is clear that $\gcd(G'_{2n}(x), d(x)) = d(x)$. For a GFP of Lucas type it holds that $G^*_0(x)$ is a non-zero constant. Since $G^*_2(x) = d(x)G^*_1(x) + g(x)G^*_0(x)$, and $\gcd(d(x), g(x)) = 1$, we have

$$\gcd(d(x), G^*_2(x)) = \gcd(d(x), d(x)G^*_1(x) + g(x)G^*_0(x)) = \gcd(d(x), g(x)G^*_0(x)) = 1.$$

Proof of part (3). We prove that $\gcd(g(x), G_1(x)) = 1$ by cases. If $G_1(x)$ is of the Fibonacci type, the conclusion is straightforward. As a second case we suppose that $G_1(x)$ is of the Lucas type. That is, $G_1(x)$ satisfies the Binet formula (4). Therefore, we have

$$\gcd(g(x), G_1(x)) = \gcd(g(x), L_1(x)) = \gcd(g(x), [a + b]/\alpha) = \gcd(g(x), d(x)/\alpha).$$

Since $\gcd(g(x), d(x)) = 1$, we have $\gcd(g(x), d(x)/\alpha) = 1$. This completes the proof. □

Lemma 2. *If $\{G_n(x)\}$ is a GFP sequence, then for every positive integer n the following holds:*

(1) $\gcd(G_n(x), G_{n+1}(x))$ *divides* $\gcd(G_n(x), g(x)G_{n-1}(x)) = \gcd(G_n(x), G_{n-1}(x))$,

(2) $\gcd(G_n(x), G_{n+2}(x))$ *divides* $\gcd(G_n(x), d(x)G_{n+1}(x))$.

Proof. We prove part (1), the proof of part (2) is similar and we omit it. If r is equal to $\gcd(G_n(x), G_{n+1}(x))$, then r divides any linear combination of $G_n(x)$ and $G_{n+1}(x)$. Therefore, $r \mid (G_{n+1}(x) - d(x)G_n(x))$. This and the recursive definition of $G_{n+1}(x)$ imply that $r \mid g(x)G_{n-1}(x)$. Therefore, $r \mid \gcd(g(x)G_{n-1}(x), G_n(x))$. Since $\gcd(g(x), G_n(x)) = 1$, we have

$$\gcd(g(x)G_{n-1}(x), G_n(x)) = \gcd(G_{n-1}(x), G_n(x)).$$

This completes the proof. □

Note that Proposition 2 part (2) when $m = n + 1$ is [12, Theorem 4].

Proposition 2. *Let m and n be positive integers with $0 < |m - n| \leq 2$.*

(1) If $G_t^*(x)$ is a GFP of Lucas type, then

$$\gcd(G_m^*(x), G_n^*(x)) = \begin{cases} G_1^*(x), & \text{if } m \text{ and } n \text{ are both odd;} \\ 1, & \text{otherwise.} \end{cases}$$

(2) If $G'_t(x)$ is a GFP of Fibonacci type, then

$$\gcd(G'_m(x), G'_n(x)) = \begin{cases} G'_2(x), & \text{if } m \text{ and } n \text{ are both even;} \\ 1, & \text{otherwise.} \end{cases}$$

Proof. We prove part (1) using several cases based on the values of m and n. The proof of part (2) is similar and we omit it. We first provide the proof for the case when m and n are consecutive integers using induction on m. Let $S(m)$ be the statement

$$\gcd(G_m^*(x), G_{m+1}^*(x)) = 1 \text{ for } m \geq 1.$$

We prove $S(1)$. From Lemma 2 part (1) we know that

$$\gcd(G_1^*(x), G_2^*(x)) \text{ divides } \gcd(G_1^*(x), g(x)G_0^*(x)). \tag{7}$$

Since

$$\gcd(G_0^*(x), G_1^*(x)) = \gcd(p_0(x), p_1(x)) = 1,$$

we have

$$\gcd(G_1^*(x), g(x)G_0^*(x)) = \gcd(G_1^*(x), g(x)).$$

This, (7), and Lemma 1 part (3) imply that $\gcd(G_1^*(x), G_2^*(x)) = 1$.

We suppose that $S(m)$ is true for $m = k - 1$. Thus, $\gcd(G_{k-1}^*(x), G_k^*(x)) = 1$. We prove that $S(k)$ is true. From Lemma 2 part (1) we know that

$$\gcd(G_k^*(x), G_{k+1}^*(x)) \text{ divides } \gcd(G_k^*(x), g(x)G_{k-1}^*(x)). \tag{8}$$

From Lemma 1 part (3) we know that $\gcd(G_k^*(x), g(x)) = 1$. Therefore,

$$\gcd(G_k^*(x), g(x)G_{k-1}^*(x)) = \gcd(G_k^*(x), G_{k-1}^*(x)).$$

This, (8), and the inductive hypothesis imply that $\gcd(G_k^*(x), G_{k+1}^*(x) = 1$.

We prove the proposition for consecutive even integers (this proof is actually a direct consequence of the previous proof). From Lemma 2 part (2), we have that $\gcd(G_{2k}^*(x), G_{2k+2}^*(x))$ divides $\gcd(G_{2k}^*(x), d(x)G_{2k+1}^*(x))$. From Lemma 1 part (2) we know that $\gcd(d(x), G_{2k}^*(x)) = 1$. This implies that

$$\gcd(G_{2k}^*(x), d(x)G_{2k+1}^*(x)) = \gcd(G_{2k}^*(x), G_{2k+1}^*(x)).$$

From the previous part of this proof –that is, the case when m and n are consecutive integers– we conclude that $\gcd(G_{2k}^*(x), G_{2k+1}^*(x)) = 1$. This proves that

$$\gcd(G_{2k}^*(x), G_{2k+2}^*(x)) = 1.$$

Finally we prove the proposition for consecutive odd integers. From the recursive definition of GFPs we have $\gcd(G_{2k+1}^*(x), G_{2k-1}^*(x))$ is equal to

$$\gcd(d(x)G_{2k}^*(x) + g(x)G_{2k-1}^*(x), G_{2k-1}^*(x)) = \gcd(d(x)G_{2k}^*(x), G_{2k-1}^*(x)).$$

From the first case in this proof we know that $\gcd(G_{2k}^*(x), G_{2k-1}^*(x)) = 1$. This implies that $\gcd(G_{2k+1}^*(x), G_{2k-1}^*(x)) = \gcd(d(x), G_{2k-1}^*(x))$. This and Lemma 1 imply that

$$\gcd(G_{2k+1}^*(x), G_{2k-1}^*(x)) = \gcd(d(x), G_{2k-1}^*(x)) = G_1^*(x).$$

This completes the proof of part (1). □

4. Identities and Other Properties of Generalized Fibonacci Polynomials

In this section we present some identities that the GFPs satisfy. These identities are required for the proofs of certain divisibility properties of the GFPs. The results in this section are proved using the Binet formulas (see Section 2). Proposition 3 part (1) is a variation of a result proved in [12], similarly Proposition 6 is a variation of a divisibility property proved by them in the same paper. A collection of this type of identities for GFPs can be found in [7].

In 1963 Ruggles [19] proved that $F_{n+m} = F_n L_m - (-1)^m F_{n-m}$. Proposition 3 parts (2) and (3) is a generalization of this numerical identity. In 1972 Hansen [9] proved that $5F_{m+n-1} = L_m L_n + L_{m-1} L_{n-1}$. Proposition 4 part (1) is a generalization of this numerical identity.

Proposition 3. *If* $\{G_n^*(x)\}$ *and* $\{G_n'(x)\}$ *are equivalent GFPs sequences, then*

(1) $G'_{m+n+1}(x) = G'_{m+1}(x)G'_{n+1}(x) + g(x)G'_m(x)G'_n(x)$,

(2) if $n \geq m$, *then* $G'_{n+m}(x) = \alpha G'_n(x)G^*_m(x) - (-g(x))^m G'_{n-m}(x)$,

(3) if $n \geq m$, *then* $G'_{n+m}(x) = \alpha G'_m(x)G^*_n(x) + (-g(x))^m G'_{n-m}(x)$.

Proof. We prove part (1). We know that $G'_n(x)$ satisfies the Binet formula (6). That is, $R_n(x) = (a^n - b^n)/(a-b)$. (Recall that we use $a := a(x)$ and $b := b(x)$.)

Therefore, $G'_{m+1}(x)G'_{n+1}(x) + g(x)G'_m(x)G'_n(x)$ is equal to,

$$\left[(a^{m+1} - b^{m+1})(a^{n+1} - b^{n+1}) + g(x)(a^m - b^m)(a^n - b^n)\right]/(a-b)^2.$$

Simplifying and factoring terms we obtain:

$$\left[\left(a^{n+m}(a^2 + g(x)) + b^{n+m}(b^2 + g(x))\right) - (a^n b^m + b^n a^m)(ab + g(x))\right]/(a-b)^2.$$

Next, since $ab = -g(x)$, we see that the above expression is equal to

$$\left[a^{n+m}(a^2 + g(x)) + b^{n+m}(b^2 + g(x))\right]/(a-b)^2.$$

This, with the facts that $(a^2 + g(x)) = a(a-b)$ and $(b^2 + g(x)) = -b(a-b)$, shows that the above expression is equal to

$$\left(a^{n+m+1} - b^{n+m+1}\right)/(a-b) = R_{n+m+1}(x).$$

This completes the proof of part (1).

We now prove part (2), the proof of part (3) is identical and we omit it. Suppose that $G^*_k(x)$ is equivalent to $G'_k(x)$ and that $G^*_k(x)$ is of the Lucas type for all k. For simplicity let us suppose that $\alpha = 1$ (the proof when $\alpha \neq 1$ is similar, so we omit it). Using the Binet formulas (4) and (6) we have that $G'_n(x)G^*_m(x) - (-g(x))^m G'_{n-m}(x)$ is equal to

$$\frac{(a^n - b^n)(a^m + b^m) - (-g(x))^m(a^{n-m} - b^{n-m})}{(a-b)}.$$

After performing the indicated multiplication and simplifying we find that this expression is equal to

$$\left[\frac{a^{n+m} - b^{n+m}}{a-b}\right] + \left[\frac{a^n b^m - a^m b^n - (-g(x))^m a^{n-m} + (-g(x))^m b^{n-m}}{a-b}\right].$$

Since $-g(x) = ab$, it is easy to see that the expression in the right bracket is equal to zero. Thus, $(a^{n+m} - b^{n+m})/(a-b) = G'_{n+m}(x)$. This completes the proof of part (2). □

Proposition 4. *Let* $\{G^*_n(x)\}$ *and* $\{G'_n(x)\}$ *be equivalent GFPs sequences. If* $m \geq 0$ *and* $n \geq 0$, *then*

(1) $(a-b)^2 G'_{m+n+1}(x) = \alpha^2 G^*_{m+1}(x) G^*_{n+1}(x) + \alpha^2 g(x) G^*_m(x) G^*_n(x)$,

(2) $G^*_{m+n+2}(x) = \alpha G^*_{m+1}(x) G^*_{n+1}(x) + g(x)[\alpha G^*_m(x) G^*_n(x) - G^*_{m+n}(x)]$.

Proof. In this proof we use $\alpha = 1$, the proof when $\alpha \neq 1$ is similar, so we omit it. (Recall, once again, that we use $a := a(x)$ and $b := b(x)$.)

Proof of part (1). Since $G^*_n(x)$ is a GFP of the Lucas type, we have that $G^*_n(x)$ satisfies the Binet formula $L_n(x) = (a^n + b^n)/\alpha$ given in (4). Therefore,

$$G^*_{m+1}(x) G^*_{n+1}(x) + g(x) G^*_m(x) G^*_n(x) \tag{9}$$

is equal to

$$\left[a^{n+1} + b^{n+1}\right]\left[a^{m+1} + b^{m+1}\right] + g(x)\left[a^n + b^n\right]\left[a^m + b^m\right].$$

Simplifying and factoring we see that this expression is equal to

$$a^{m+n}\left[a^2 + g(x)\right] + b^{m+n}\left[b^2 + g(x)\right] + (ab + g(x))\left[a^m b^n + a^n b^m\right].$$

Since

$$ab = -g(x),\ a^2 + g(x) = a(a-b),\ \text{and } b^2 + g(x) = -b(a-b),$$

the expression in (9) is equal to $(a-b)(a^{m+n+1} - b^{m+n+1})$. We recall that $G'_{m+n+1}(x)$ is equivalent to $G^*_{m+n+1}(x)$. Thus, $G'_{m+n+1}(x) = (a^{m+n+1} - b^{m+n+1})/(a-b)$. Therefore, $(a-b)^2 G'_{m+n+1}(x) = (a-b)\left[a^{m+n+1} - b^{m+n+1}\right]$. This completes the proof of part (1).

Proof of part (2). From the proof of part (1) we know that

$$(a-b)^2 G'_{m+n+1}(x) = (a-b)[a^{m+n+1} - b^{m+n+1}].$$

Simplifying the right side of the previous equality we have

$$(a-b)^2 G'_{m+n+1}(x) = a^{m+n+2} - ba^{m+n+1} - ab^{m+n+1} + b^{m+n+2}.$$

So, $(a-b)^2 G'_{m+n+1}(x) = a^{m+n+2} + b^{m+n+2} - ab[a^{m+n} + b^{m+n}]$. We recall that $ab = -g(x)$. Thus,

$$(a-b)^2 G'_{m+n+1}(x) = a^{m+n+2} + b^{m+n+2} + g(x)[a^{m+n} + b^{m+n}].$$

This and the Binet formula (4) imply that

$$(a-b)^2 G'_{m+n+1}(x) = G^*_{m+n+2}(x) + g(x) G^*_{m+n}(x).$$

So, the proof follows from part (1) of this proposition. □

Proposition 5. *Let $\{G^*_n(x)\}$ be a GFP sequence of the Lucas type. If m, n, r, and q are positive integers, then*

(1) if $m \leq n$*, then* $G^*_{m+n}(x) = \alpha G^*_m(x)G^*_n(x) + (-1)^{m+1}(g(x))^m G^*_{n-m}(x)$.

(2) If $r < m$*, then there is a polynomial* $T(x)$ *such that*

$$G^*_{mq+r}(x) = \begin{cases} G^*_m(x)T(x) + (-1)^{w+t}(g(x))^w G^*_{m-r}(x), & \text{if } q \text{ is odd;} \\ G^*_m(x)T(x) + (-1)^{(m+1)t}(g(x))^{mt} G^*_r(x), & \text{if } q \text{ is even} \end{cases}$$

where $t = \left\lceil \frac{q}{2} \right\rceil$ *and* $w = (t-1)m + r$.

(3) If $n > 1$*, then there is a polynomial* $T_n(x)$ *such that*

$$G^*_{2^n r}(x) = G^*_r(x)T_n(x) + (2/\alpha)(g(x))^{2^{n-1}r}.$$

Proof. We prove part (1). Since $G^*_m(x)$ and $G^*_n(x)$ are of the Lucas type, they both satisfy the Binet formula (4). Thus,

$$G^*_m(x)G^*_n(x) = \left(\frac{a^m + b^m}{\alpha}\right)\left(\frac{a^n + b^n}{\alpha}\right) = \frac{a^{m+n} + b^{m+n}}{\alpha^2} + \frac{(ab)^m\left(a^{n-m} + b^{n-m}\right)}{\alpha^2}.$$

So, $G^*_m(x)G^*_n(x) = \left[G^*_{n+m}(x) + (ab)^m G^*_{n-m}(x)\right]/\alpha$. This and $ab = -g(x)$ imply that

$$G^*_{m+n}(x) = \alpha G^*_m(x)G^*_n(x) - (-g(x))^m G^*_{n-m}(x).$$

This completes the proof of part (1).

We prove part 2 using cases and mathematical induction.

`Case` q `is odd`. Suppose $q = 2t - 1$, and let $S(t)$ be the following statement. For every positive integer t there is a polynomial $T_t(x)$ such that

$$G^*_{m(2t-1)+r}(x) = G^*_m(x)T_t(x) + (-1)^{m(t-1)+t+r}(g(x))^{(t-1)m+r} G^*_{m-r}(x).$$

From part (1), taking $T_1(x) = \alpha G^*_r(x)$, it is easy to see that $S(t)$ is true if $t = 1$.

We suppose that $S(k)$ is true. That is, suppose that there is a polynomial $T_k(x)$ such that

$$G^*_{m(2k-1)+r}(x) = G^*_m(x)T_k(x) + (-1)^{m(k-1)+t+r}(g(x))^{(k-1)m+r} G^*_{m-r}(x). \quad (10)$$

We prove that $S(k+1)$ is true. Notice that $G^*_{m(2k+1)+r}(x) = G^*_{(2km+r)+m}(x)$. Therefore, from part (1) we have

$$G^*_{m(2k+1)+r}(x) = \alpha G^*_m(x)G^*_{2km+r}(x) + (-1)^{m+1} g^m(x) G^*_{m(2k-1)+r}(x).$$

This and $S(k)$ (see (10)) imply that

$$G^*_{m(2k+1)+r}(x) = \alpha G^*_m(x)G^*_{2km+r}(x) + (-1)^{m+1}(g(x))^m G^*_m(x)T_k(x) + M_1(x)$$

where $M_1(x) = (-1)^{km+(t+1)+r}(g(x))^{km+r}G^*_{m-r}(x)$. Therefore, $G^*_{m(2k+1)+r}(x)$ is equal to

$$G^*_m(x)[\alpha G^*_{2km+r}(x)+(-1)^{m+1}(g(x))^m T_k(x)]+(-1)^{km+(t+1)+r}(g(x))^{km+r}G^*_{m-r}(x).$$

This, with $T_{k+1}(x) := \alpha G^*_{2km+r}(x) + (-1)^{m+1}(g(x))^m T_k(x)$, implies $S(k+1)$. This completes the proof when q is odd.

`Case` q `is even`. This proof is similar to the case in which q is odd. Suppose $q = 2t$, and let $H(t)$ be the following statement. For every positive integer there is a polynomial $T_t(x)$ such that

$$G^*_{m(2t)+r}(x) = G^*_m(x)T_t(x) + (-1)^{(m+1)t}(g(x))^{mt}G^*_r(x).$$

From part (1), taking $T_1(x) = \alpha G^*_r(x)$, it is easy to see that $H(t)$ is true if $t = 1$.

We suppose that $H(k)$ is true. That is, suppose that there is a polynomial $T_k(x)$ such that

$$G^*_{m(2k)+r}(x) = G^*_m(x)T_k(x) + (-1)^{(m+1)k}(g(x))^{mk}G^*_r(x). \tag{11}$$

We prove that $H(k+1)$ is true. Notice that $G^*_{2m(k+1)+r}(x) = G^*_{((2k+1)m+r)+m}(x)$. Therefore, from part (1) we have

$$G^*_{2m(k+1)+r}(x) = \alpha G^*_m(x)G^*_{(2k+1)m+r}(x) + (-1)^{m+1}(g(x))^m G^*_{2mk+r}(x).$$

This and $H(k)$ (see (11)) imply that

$$G^*_{m(2(k+1))+r}(x) = \alpha G^*_m(x)G^*_{(2k+1)m+r}(x) + (-1)^{m+1}(g(x))^m G^*_m(x)T_k(x) + M_2(x)$$

where $M_2(x) = (-1)^{(k+1)(m+1)}(g(x))^{m(k+1)}G^*_r(x)$. Therefore,

$$G^*_{m(2(k+1))+r}(x) = G^*_m(x)\left[\alpha G^*_{(2k+1)m+r}(x) + (-1)^{m+1}(g(x))^m T_k(x)\right] + M_2(x).$$

This, with $T_{k+1}(x) := \alpha G^*_{(2k+2)m+r}(x) + (-1)^m(g(x))^m T_k(x)$, implies $H(k+1)$.

We finally prove part (3) by induction. Since $G^*_n(x)$ is of the Lucas type, by the Binet formula it is easy to see that $G_0(x) = 2/\alpha$. Let $S(n)$ be the statement: for every positive integer n there is a polynomial $T_n(x)$ such that this equality holds $G^*_{2^n r}(x) = G^*_r(x)T_n(x) + (2/\alpha)g^{2^{n-1}r}(x)$.

Proof of $S(2)$. From part (1) we have

$$G^*_{2^2 r}(x) = G^*_{2r+2r}(x) = \alpha(G^*_{2r}(x))^2 - (2/\alpha)(g(x))^{2r}.$$

Applying the result in part (1) for $G^*_{2r}(x)$ again (and simplifying) we obtain:

$$\begin{aligned} G^*_{2^2 r}(x) = {} & \alpha[\alpha(G^*_r(x))^2 - \frac{2}{\alpha}(-g(x))^r]^2 - \frac{2}{\alpha}(g(x))^{2r} \\ = {} & G^*_r(x)[(\alpha G^*_r(x))^3 - (-1)^r 4\alpha G^*_r(x)(g(x))^r] + \tfrac{4(g(x))^{2r}-2(g(x))^{2r}}{\alpha} \\ = {} & G^*_r(x)T_2(x) + \frac{2}{\alpha}(g(x))^{2r} \end{aligned}$$

where $T_2(x) = \alpha^3(G^*_r(x))^3 + (-1)^{r+1}4\alpha G^*_r(x)(g(x))^r$. This proves $S(2)$.

We suppose that $S(k)$ is true for $k > 2$, and we prove $S(k+1)$ is true. That is, we suppose that for a fixed k there is a polynomial $T_k(x)$ such that

$$G^*_{2^k r}(x) = G^*_r(x)T_k(x) + (2/\alpha)g^{2^{k-1}r}(x).$$

From part (1) we have $G^*_{2^{k+1}r}(x) = G^*_{2^k r+2^k r}(x) = \alpha(G^*_{2^k r}(x))^2 - (2/\alpha)(g(x))^{2^k r}$. Using the result from the inductive hypothesis $S(k)$ and simplifying, we obtain:

$$\begin{aligned} G^*_{2^{k+1}r}(x) &= \alpha[G^*_r(x)T_k(x) + \frac{2}{\alpha}(g(x))^{2^{k-1}r}]^2 - \frac{2}{\alpha}(g(x))^{2^k r} \\ &= G^*_r(x)[\alpha G^*_r(x)T_k^2(x) + 4T_k(x)(g(x))^{2^{k-1}r}] + \tfrac{4(g(x))^{2^k r} - 2(g(x))^{2^k r}}{\alpha} \\ &= G^*_r(x)T_{k+1}(x) + \frac{2}{\alpha}(g(x))^{2^k r} \end{aligned}$$

where $T_{k+1}(x) = \alpha G^*_r(x)T_k^2(x) + 4T_k(x)(g(x))^{2^{k-1}r}$. This completes the proof of part (3). □

In the following part of this section, we present two divisibility properties for the GFPs. Proposition 6 is [12, Theorem 6].

Proposition 6. *If $\{G'_n(x)\}$ is a GFP sequence of the Fibonacci type, then $G'_m(x)$ divides $G'_n(x)$ if and only if m divides n.*

Proof. We first prove the sufficiency. Based on the hypothesis that m divides n, there is an integer $q \geq 1$ such that $n = mq$. Then, using the Binet formula (6), we have

$$G'_m(x) = (a^m - b^m)/(a-b) \quad \text{and} \quad G'_{mq}(x) = (a^{mq} - b^{mq})/(a-b).$$

It is easy to see, using induction on q, that $(a^m - b^m)$ divides $(a^{mq} - b^{mq})$ which implies that $G'_m(x)$ divides $G'_{mq}(x)$. This proves the sufficiency.

We now prove the necessity. Suppose that m does not divide n and that $G'_m(x)$ divides $G'_n(x)$ for m and n greater than 1. Therefore, there are integers q and r with $0 < r < n$ such that $n = mq + r$. Then by Proposition 3 part (1)

$$\begin{aligned} G'_n(x) &= G'_{mq+r}(x) \\ &= G'_{mq+1}(x)G'_r(x) + g(x)G'_{mq}(x)G'_{r-1}(x) \\ &= \left(d(x)G'_{mq}(x) + g(x)G'_{mq-1}(x)\right)G'_r(x) + g(x)G'_{mq}(x)G'_{r-1}(x) \\ &= d(x)G'_{mq}(x)G'_r(x) + g(x)G'_{mq-1}(x)G'_r(x) + g(x)G'_{mq-1}(x)G'_r(x). \end{aligned}$$

Grouping terms and simplifying we obtain

$$G'_n(x) = G'_{mq}(x)G'_{r+1}(x) + g(x)G'_{mq-1}(x)G'_r(x).$$

This and the fact that $G'_m(x) \mid G'_n(x)$ and $G'_m(x) \mid G'_{mq}(x)$ imply that

$$G'_m(x) \mid g(x)G'_{mq-1}(x)G'_r(x).$$

From Lemma 1 part (3) and Proposition 2 we know that $\gcd(G'_{mq}(x), g(x)) = 1$ and that $\gcd(G'_{mq-1}(x), G'_{mq}(x)) = 1$, respectively. These two facts imply that $G'_m(x) \mid G'_r(x)$. That is a contradiction since degree $(G'_{r-1}(x)) <$ degree $(G'_{m-1}(x))$. This completes the proof. □

The following corollary gives a factorization of a GPF of Fibonacci type $G'_n(x)$. It is a direct application of Theorem 6 and some results given in articles by Bliss, et al. and Nowicki [3, 23]. In fact, the proof of Corollary 1 follows from Theorem 6 and [23, Theorem 2], so we omit the details. We start by giving a short background of the lcm sequences for polynomials that fits the context of this paper, a more general result can be found in [23]. If lcm denotes the least common multiple, then we define $c_n(x)$ recursively as follows: Let $c_1 = 1$ and

$$c_n(x) = \frac{\operatorname{lcm}(G'_1(x), G'_2(x), \ldots, G'_n(x))}{\operatorname{lcm}(G'_1(x), G'_2(x), \ldots, G'_{n-1}(x))} \quad \text{for } n \geq 2.$$

Corollary 1. *If $G'_n(x)$ is a GFP of Fibonacci type, then $G'_n(x) = \prod_{d|n} c_d(x)$.*

The factors c_i are not always irreducible polynomials. For instance, if $G'_{10}(x)$ is a Chebyshev polynomial of the first kind, then its irreducible factoring is

$$G'_{10}(x) = 2x(-1 - 2x + 4x^2)(-1 + 2x + 4x^2)(5 - 20x^2 + 16x^4).$$

Using Corollary 1 we have

$$\begin{aligned} G'_{10}(x) &= c_1(x)c_2(x)c_5(x)c_{10}(x) \\ &= (1)(2x)(1 - 12x^2 + 16x^4)(5 - 20x^2 + 16x^4). \end{aligned}$$

Proposition 7. *Let m be a positive integer that is not a power of two. If $G^*_m(x)$ is a GFP of Lucas type, then for all odd divisors q of m, it holds that $G^*_{m/q}(x)$ divides $G^*_m(x)$. Moreover $G^*_{m/q}(x)$ is of the Lucas type.*

Proof. Let q be an odd divisor of m. If $q = 1$ the result is obvious. Let us suppose that $q \neq 1$. Therefore, there is an integer $d > 1$ such that $m = dq$. Using the Binet formula (4), where $a := a(x)$ and $b := b(x)$, we have $G^*_m(x) = G^*_{dq}(x) = (a^{dq} + b^{dq})/\alpha$. Let $X = a^d$ and $Y = b^d$. Using induction it is possible to prove that $X + Y$ divides $X^q + Y^q$. This implies that there is a polynomial $Q(x)$ such that $(X^q + Y^q)/\alpha = Q(x)(X + Y)/\alpha$. Therefore,

$$G^*_m(x) = G^*_{dq}(x) = (a^{dq} + b^{dq})/\alpha = Q(x)(a^d + b^d)/\alpha.$$

This and the Binet formula (4) imply that $G^*_m(x) = G^*_d(x)Q(x)$. □

5. Characterization of the Strong Divisibility Property

In this section we prove the main results of this paper. Thus, we prove a necessary and sufficient condition for the strong divisibility property for GFPs of Fibonacci type. We also prove that the strong divisibility property holds partially for GFPs of Lucas type. The other important result in this section is that the strong divisibility property holds partially for a GFP and its equivalent. The results here therefore provide a complete characterization of the strong divisibility property satisfied by the GFPs of Fibonacci type.

We note that if $G^*_m(x)$ and $G'_n(x)$ are two equivalent polynomials from Table 2, then $\gcd(G^*_m(x), G'_n(x))$ is either $G^*_{\gcd(m,n)}(x)$ or one. However, it is not true in general. Here we give an example of a pair of GFPs that do not satisfy this property. First we define a Fibonacci type polynomial

$$G'_0(x) = 0,\ G'_1(x) = 1,\ \text{and}\ G'_n(x) = (2x+1)G'_{n-1}(x) + G'_{n-2}(x)\ \text{for}\ n \geq 2.$$

We now define its equivalent polynomial of the Lucas type

$$G^*_0(x) = 2,\ G^*_1(x) = 2x+1,\ \text{and}\ G^*_n(x) = (2x+1)G^*_{n-1}(x) + G^*_{n-2}(x)\ \text{for}\ n \geq 2.$$

After some calculations we see that $\gcd(G^*_m(x), G'_n(x))$ is one, two, or $G^*_{\gcd(m,n)}(x)$. Using the same polynomials we can also see that $\gcd(G^*_m(x), G^*_n(x))$ is one, two, or $G^*_{\gcd(m,n)}(x)$. If we do the same calculations for numerical sequences (Fibonacci and Lucas numbers), we can see that they have the same behavior.

In this section we use the notation $E_2(n)$ to represent the *integer exponent base two* of a positive integer n which is defined to be the largest integer k such that $2^k \mid n$.

Lemma 3. *If $R(x)$, $S(x)$, and $T(x)$ are polynomial in $\mathbb{Z}[x]$, then*

$$\gcd(R(x), T(x)) = \gcd(R(x), R(x)S(x) - T(x)).$$

Proposition 8. *Let $\{G^*_n(x)\}$ be a GFP sequence of the Lucas type. If $m \mid n$ and $E_2(n) = E_2(m)$, then $\gcd(G^*_n(x), G^*_m(x)) = G^*_m(x)$.*

Proof. First we recall that $E_2(n)$ is the largest integer k such that $2^k \mid n$. We suppose that $n = mq$ with $q \in \mathbb{N}$. Since $E_2(m) = E_2(n) = E_2(mq)$, we conclude that q is odd. This, Lemma 3, and Proposition 5 part (2) imply that

$$\begin{aligned}
\gcd(G^*_n(x), G^*_m(x)) &= \gcd(G^*_{qm}(x), G^*_m(x)) \\
&= \gcd(G^*_m(x)T(x) + (-1)^n(-g(x))^{(n-1)m}G^*_m(x), G^*_m(x)) \\
&= G^*_m(x).
\end{aligned}$$

This proves the proposition. □

Corollary 2. *Let $G^*_m(x)$ be a GFP of Lucas type. If $m > 0$ is not a power of two, then for all odd divisors q of m, it follows that $G^*_{m/q}(x)$ divides $G^*_m(x)$. More over $G^*_{m/q}(x)$ is of the Lucas type.*

Proof. It is easy to see that $E_2(m/q) = E_2(m)$. Therefore, the conclusion follows by Proposition 8. □

Proposition 9. *Let $d_k = \gcd(G^*_0(x), G^*_k(x))$ where $G^*_k(x)$ is a GFP of the Lucas type. Suppose that there is an integer $k' > 0$ such that $d_{k'} = 2$. If m is the minimum positive integer such that $d_m = 2$, then $m|n$ if and only if $d_n = 2$.*

Proof. We suppose that m is the minimum positive integer such that $d_m = 2$. Let $m|n$, by Proposition 8 we know that $\gcd(G^*_m(x), G^*_n(x)) = G^*_m(x)$ (we recall that $G^*_0(x) = p_0(x)$ and $|p_0(x)| = 1$ or 2). This and the fact that $2|G^*_m(x)$ imply that $\gcd(G^*_0(x), G^*_n(x)) = 2$. This proves that $d_n = 2$.

We note that $2|\gcd(G^*_m(x), G^*_n(x))$. Suppose that there is a $n \in \mathbb{N} - \{m\}$ that satisfies the condition $d_n = 2$. From the division algorithm we have that there are integers q and r such that $n = mq + r$ where $0 \leq r < m$. This and Proposition 5 part (2) imply that

$$\gcd(G^*_m(x), G^*_n(x)) = \begin{cases} \gcd(G^*_m(x), (g(x))^{(t-1)m+r} G^*_{m-r}(x)), & \text{if q is odd;} \\ \gcd(G^*_m(x), (g(x))^{mt} G^*_r(x)), & \text{if q is even.} \end{cases}$$

This and Lemma 1 part (3) imply that $\gcd(G^*_m(x), G^*_n(x))$ is either

$$\gcd(G^*_m(x), G^*_r(x)) \quad \text{or} \quad \gcd(G^*_m(x), G^*_{m-r}(x)).$$

From this and the fact that $2|\gcd(G^*_m(x), G^*_n(x))$, we conclude that either

$$\gcd(G^*_r(x), G^*_0(x)) = 2 \quad \text{or} \quad \gcd(G^*_{m-r}(x), G^*_0(x)) = 2.$$

This holds only if $r = 0$, due to definition of m. Therefore, $n = mq$. □

Lemma 4. *Let $G^*_k(x)$ be a GFP of Lucas type and let $n = mq + r$ where m, q and r are positive integers with $r < m$. If $m_1 = m - r$ when q is odd and $m_1 = r$ when q is even, then $\gcd(G^*_n(x), G^*_m(x)) = \gcd(G^*_{m_1}(x), G^*_m(x))$.*

Proof. Let

$$f(x) = \begin{cases} (-1)^{m(t-1)+t+r} (g(x))^{(t-1)m+r}, & \text{if } q \text{ is odd;} \\ (-1)^{(m+1)t} (g(x))^{mt}, & \text{if } q \text{ is even.} \end{cases}$$

This and Lemma 1 part (3) imply that $\gcd(G^*_m(x), f(x)) = 1$. Therefore, by Proposition 5 part (2) it follows that

$$\gcd(G^*_{mq+r}(x), G^*_m(x)) = \gcd(G^*_m(x)T(x) + f(x)G^*_{m_1}(x), G^*_m).$$

Now it is easy to see that

$$\gcd(G_m^*(x)T(x) + f(x)G_{m_1}^*(x), G_m^*) = \gcd(f(x)G_{m_1}^*(x), G_m^*(x)).$$

Since $\gcd(G_m^*(x), f(x)) = 1$, by Proposition 1 part (1) we have

$$\gcd(f(x)G_{m_1}^*(x), G_m^*(x)) = \gcd(G_{m_1}^*(x), G_m^*(x)).$$

This completes the proof. □

Theorem 1. *Let $G_n^*(x)$ be a GFP of the Lucas type. If m and n are positive integers and $d = \gcd(m, n)$, then*

$$\gcd(G_m^*(x), G_n^*(x)) = \begin{cases} G_d^*(x), & \text{if } E_2(m) = E_2(n); \\ \gcd(G_d^*(x), G_0^*(x)), & \text{otherwise.} \end{cases}$$

Proof. First we prove the result for $E_2(n) = E_2(m)$. From the Euclidean algorithm we know that there are non-negative integers q and r such that $n = mq + r$ with $r < m$. Let $d = \gcd(m, n)$. Clearly, if $r = 0$, then $d = m$. Therefore, the result holds by Proposition 8.

We suppose that $r \neq 0$. If we take m_1 as in Lemma 4, then

$$\gcd(G_n^*(x), G_m^*(x)) = \gcd(G_{mq+r}^*(x), G_m^*(x)) = \gcd(G_{m_1}^*(x), G_m^*(x)).$$

Let $M_1 = \{m, m_1\}$. Notice that $\gcd(m_1, m) = d$, $E_2(m) = E_2(m_1)$, and that $m_1 < m$. Therefore, there are non-negative integers q_1 and r_1 such that $m = m_1q_1 + r_1$ with $r_1 < m_1$. Again, if $r_1 = 0$, by Proposition 8 we obtain that $\gcd(G_n^*(x), G_m^*(x)) = \gcd(G_m^*(x), G_{m_1}^*(x)) = G_d^*(x)$. If $r_1 \neq 0$ we repeat the previous step and then we can guarantee that

$$\gcd(G_n^*(x), G_m^*(x)) = \gcd(G_{m_1}^*(x), G_m^*(x)) = \gcd(G_{m_1}^*(x), G_{m_2}^*(x)),$$

where

$$m_2 = \begin{cases} m_1 - r_1, & \text{if } q \text{ is odd;} \\ r_1, & \text{if } q \text{ is even.} \end{cases}$$

We repeat this procedure t times until we obtain the ordered decreasing sequence $m > m_1 > m_2 > \cdots > m_t \geq d$ such that $E_2(m) = E_2(m_t)$ and $\gcd(m_t, m_{t-1}) = d$, where

$$m_t = \begin{cases} m_{t-1} - r_{t-1}, & \text{if } q \text{ is odd;} \\ r_{t-1}, & \text{if } q \text{ is even.} \end{cases}$$

Notice that $M_t = \{m, m_1, m_2, \ldots, m_t\} = M_{t-1} \cup \{m_t\}$ is an ordered set of natural numbers, therefore there is a minimum element. Since M_t is constructed with a sequence of decreasing positive integers, there must be an integer k such that

$M_t \subset M_k$ for all $t < k$ and M_{k+1} is undefined. Thus, the procedure ends with M_k. Note that $m > m_1 > m_2 > \cdots > m_k \geq d$ such that $E_2(m) = E_2(m_k)$ and $\gcd(m_k, m_{k-1}) = d$.

Claim. The minimum element of M_k is $m_k = d$ and $m_k \mid m_{k-1}$.

Proof of claim. From the division algorithm we know that there are non-negative integers q_k and r_k such that $m_{k-1} = m_k q_k + r_k$ with $r_k < m_k$. If $r_k \neq 0$ we can repeat the procedure described above to obtain a new set M_{k+1} with $M_k \subset M_{k+1}$. That is a contradiction. Therefore, $r_k = 0$. So, $m_{k-1} = m_k q_k$. This implies that $\gcd(m_k, m_{k-1}) = d$. Thus, $m_k = d$. This proves the claim.

The Claim and Proposition 8 allow us to conclude that

$$\gcd(G_n^*(x), G_m^*(x)) = \gcd(G_m^*(x), G_{m_1}^*(x)) = \cdots = \gcd(G_{m_{k-1}}^*(x), G_{m_k}^*(x)) = G_d^*.$$

We now prove by cases that: if $E_2(n) \neq E_2(m)$ and $d = \gcd(n, m)$, then $\gcd(G_n^*(x), G_m^*(x)) = \gcd(G_d^*(x), G_0^*(x))$.

`Case 1.` Suppose that $m < n$ and that $E_2(n) < E_2(m)$. From the division algorithm there are two non-negative integers q and r such that $n = mq + r$ with $r < m$. Let $m_1 = m - r$ when q is odd and $m_1 = r$ when q is even (as defined in Lemma 4). Since $n = mq + r$ and $E_2(n) < E_2(m)$, we have $r \neq 0$. It is easy to see that $E_2(n) = E_2(r)$, and therefore $E_2(n) = E_2(m_1)$. This and Lemma 4 imply that $\gcd(G_n^*(x), G_m^*(x)) = \gcd(G_m^*(x), G_{m_1}^*(x))$. Since $E_2(m_1) = E_2(n) < E_2(m)$ and $m_1 < m$, the criteria for the Case 2 are satisfied here, so the proof of this case may be completed as we are going to do in Case 2 below.

`Case 2.` Suppose that $E_2(m) < E_2(n)$ and that $m < n$. From the division algorithm we know that there are two non-negative integers r and q such that $n = mq+r$ with $r < m$. If $r = 0$, then q must be even (because $E_2(m) < E_2(n)$). Let $k = E_2(q)$ and we consider two subcases on k.

`Subcase 1.` If $k = 1$, then $q = 2t$ where t is odd. Therefore, by Proposition 5 part (1) we have $G_n^*(x) = G_{2mt}^*(x) = \alpha(G_{mt}^*(x))^2 + (-1)^{mt+1}(G_0^*(x))(-g(x))^{mt}$. This, Proposition 8, Lemma 1 part (3), and Lemma 3 imply that

$$\begin{aligned}
\gcd(G_n^*(x), G_m^*(x)) &= \gcd\left(\alpha(G_{mt}^*(x))^2 + (-1)^{mt+1} G_0^*(x)(-g(x))^{mt}, G_m^*(x)\right) \\
&= \gcd((-1)^{mt+1} G_0^*(x)(-g(x))^{mt}, G_m^*(x)) \\
&= \gcd(G_0^*(x), G_m^*(x)) \\
&= \gcd(G_0^*(x), G_d^*(x)).
\end{aligned}$$

`Subcase 2.` If $k > 1$, then $q = 2^k t$ where t is odd. Therefore, by Proposition 5 part (3), there is a polynomial $T_k(x)$ such that

$$G_n^* = G_{2^k mt}^* = G_{mt}^*(x) T_k(x) + G_0^*(x) g^{2^{k-1} mt}(x).$$

This, Proposition 8, Lemma 1 part (3), and Lemma 3 imply that

$$\begin{aligned}\gcd(G^*_n(x), G^*_m(x)) &= \gcd(G^*_{mt}(x)T_k(x) + G^*_0(x)g^{2^{k-1}mt}(x), G^*_m(x))\\ &= \gcd(G^*_0(x)g^{2^{k-1}mt}(x), G^*_m(x))\\ &= \gcd(G^*_0(x), G^*_m(x))\\ &= \gcd(G^*_0(x), G^*_d(x)).\end{aligned}$$

Now suppose that $r \neq 0$. This and Lemma 4 imply that

$$\gcd(G^*_n(x), G^*_m(x)) = \gcd(G^*_m(x), G^*_{m_1}(x)),$$

where $m_1 = m - r$ when q is odd and $m_1 = r$ when q is even (as defined in Lemma 4). Therefore, $m_1 < m < n$ and $\gcd(m, n) = \gcd(m, m_1) = d$.

We analyze both the case in which $m_1 \mid m$ and the case in which $m_1 \nmid m$. Suppose that $m = m_1q_2$ and we consider two cases for q_2.

`Subcase` q_2 `is odd.` If q_2 is odd then we have $E_2(m_1) = E_2(m)$. Therefore, by Proposition 8 we obtain:

$$\gcd(G^*_m(x), G^*_n(x)) = \gcd(G^*_m(x), G^*_{m_1}(x)) = G^*_d(x) \quad\text{and}\quad E_2(G^*_d(x)) < E_2(G^*_n(x)).$$

This implies that $\gcd(G^*_m(x), G^*_n(x)) = \gcd(G^*_d(x), G^*_0(x))$.

`Subcase` q_2 `is even.` If q_2 is even, then $E_2(m_1) < E_2(m)$. Now it is easy to see that $\gcd(G^*_m(x), G^*_n(x)) = \gcd(G^*_{m_1}(x), G^*_0(x)) = \gcd(G^*_d(x), G^*_0(x))$.

Now suppose that $m_1 \nmid m$. Therefore there are two non-negative integers r_2 and q_2 such that $m = m_1q_2 + r_2$ where $0 < r_2 < m_1$. From Lemma 4 we guarantee that we can find m_2 such that

$$m_2 < m_1, \gcd(m_1, m_2) = d \quad\text{and}\quad \gcd(G^*_{m_1}(x), G^*_{m_2}(x)) = \gcd(G^*_{m_1}(x), G^*_m(x)).$$

In this way we construct an ordered set of integers $M_t = \{n, m, m_1, m_2, \ldots, m_t\}$ where $n > m > m_1 > \cdots > m_t$ such that $\gcd(m_j, m_{j-1}) = d$ and

$$\gcd(G^*_n(x), G^*_m(x)) = \gcd(G^*_{m_1}(x), G^*_m(x)) = \cdots = \gcd(G^*_{m_j}(x), G^*_{m_{j-1}}(x)).$$

From Lemma 4 we know that $n > m > m_1 > \cdots > m_j$ ends only if $r_j = 0$. Since $M_j = \{n, m, m_1, m_2, \ldots, m_j\}$ is an ordered sequence of natural numbers, it has a minimum element m_j. Therefore, $m_j \mid m_{j-1}$. It is easy then to see that

$$\gcd(G^*_n(x), G^*_m(x)) = \gcd(G^*_{m_j}(x), G^*_{m_{j-1}}(x)).$$

This is equivalent to $\gcd(G^*_n(x), G^*_m(x)) = \gcd(G^*_d(x), G^*_0(x))$, which completes the proof. □

Corollary 3. *Let* $d_k = \gcd(G_0^*(x), G_k^*(x))$ *where* $G_k^*(x)$ *is a GFP of the Lucas type. If* m *and* n *are positive integers such that* $E_2(n) \neq E_2(n)$*, then the following properties hold*

(1) Suppose that there is an integer $k' > 0$ *such that* $d_{k'} = 2$*. If* r *is the minimum positive integer such that* $d_r = 2$*, then*

$$\gcd(G_m^*(x), G_n^*(x)) = \begin{cases} 2, & \text{if } r \mid \gcd(m,n); \\ 1, & \text{otherwise.} \end{cases}$$

(2) If $d_k \neq 2$ *for every positive integer* k*, then* $\gcd(G_m^*(x), G_n^*(x)) = 1$.

The proof of this corollary is straightforward from Proposition 9.

Proposition 10. *Let* $G_n^*(x)$ *and* $G'_n(x)$ *be equivalent GFPs. If* m *and* n *are positive integers, then*

(1) $\gcd(G'_{m+n+1}(x), G_n^*(x)) = \gcd(G_{m+1}^*(x), G_n^*(x))$,

(2) if $m > n$*, then* $\gcd(G'_{m-n+1}(x), G_n^*(x)) = \gcd(G_{m+1}^*(x), G_n^*(x))$,

(3) if $m < n$*, then* $\gcd(G'_{n-m+1}(x), G_n^*(x)) = \gcd(G_{m-1}^*(x), G_n^*(x))$.

Proof. We prove part (1) by induction. Let $S(n)$ be the statement (recall that $a-b = a(x) - b(x)$): for every $n \geq 1$, $\gcd((a-b)^2, G_n^*(x)) = 1$. Recall that in a GFP of Lucas type, $\gcd(p_0(x), p_1(x)) = \gcd(p_0(x), d(x)) = 1$ and that $2p_1(x) = p_0(x)d(x)$. From this and Proposition 4 part (1) with $m = n = 0$, it is easy to see that $\gcd((a-b)^2, G_1^*(x)) = 1$. We now prove that $S(2)$ is also true. It is easy to see that

$$\begin{aligned} \gcd((a-b)^2, G_2^*(x)) &= \gcd(a^2(x) + b^2(x) - 2ab, G_2^*(x)) \\ &= \gcd(G_2^*(x) + 2g(x), G_2^*(x)) \\ &= \gcd(2g(x), G_2^*(x)). \end{aligned}$$

From Lemma (1) part (3) we know that $\gcd(g(x), G_2^*(x)) = 1$. This implies that either

$$\gcd((a-b)^2, G_2^*(x)) = 1 \quad \text{or} \quad \gcd((a-b)^2, G_2^*(x)) = 2.$$

If $\gcd((a-b)^2, G_2^*(x)) = 2$, then $2 \mid \left(d^2(x) + 4g(x)\right)$ and $2 \mid G_2^*(x)$. So, $2 \mid d^2(x)$ and $2 \mid G_2^*(x)$. From Lemma (1) part (2) we know that $\gcd(d(x), G_2^*(x)) = 1$. This implies that $2 \mid 1$. Therefore, $\gcd((a-b)^2, G_2^*(x)) = 1$. This proves $S(2)$.

Suppose that $S(k)$ is true. Then $\gcd((a-b)^2, G_k^*(x)) = 1$. We now prove that $S(k+1)$ is true. Suppose we have $\gcd((a-b)^2, G_{k+1}^*(x)) = r(x)$. Therefore,

$r(x) \mid (a-b)^2$ and $r(x) \mid G^*_{k+1}(x)$. So, $r(x) \mid [(a-b)^2 G'_{2k+1}(x) - \alpha^2 (G^*_{k+1}(x))^2]$. From Proposition 4 part (1) we know that if $m = n = k$, then

$$(a-b)^2 G'_{k+k+1}(x) = \alpha^2 G^*_{k+1}(x) G^*_{k+1}(x) + \alpha^2 g(x) G^*_k(x) G^*_k(x).$$

Thus, $(a-b)^2 G'_{2k+1}(x) - \alpha^2 (G^*_{k+1}(x))^2 = \alpha^2 g(x)(G^*_k(x))^2$. This implies that $r(x)$ divides $\alpha^2 g(x)(G^*_k(x))^2$. Since $|\alpha| = 1$ or 2, from the definition of GFPs and Proposition 2 it is easy to see that $\gcd(\alpha, g(x)) = 1$. We know that $\gcd(\alpha, G_n) = 1$ for every n. So, $\gcd(\alpha, r(x)) = 1$. We recall from Lemma (1) part (3) that $\gcd(g(x), G^*_{k+1}(x)) = 1$. This and $r(x) \mid G^*_{k+1}(x)$ imply that $\gcd(r(x), g(x)) = 1$. Now it is easy to see that $r(x) \mid (G^*_k(x))^2$. Since $\gcd((a-b)^2, G^*_k(x)) = 1$ and $r(x) \mid (a-b)^2$, we have $r(x) = 1$. This proves that $S(k+1)$ is true. That is, $\gcd((a-b)^2, G^*_n(x)) = 1$.

We now prove that $\gcd(G'_{m+n+1}(x), G^*_n(x)) = \gcd(G^*_{m+1}(x), G^*_n(x))$. Proposition 4 part (1), implies that $\gcd((a-b)^2 G'_{m+n+1}(x), G^*_n(x))$ is equal to

$$\gcd(\alpha^2 G^*_{m+1}(x) G^*_{n+1}(x) + \alpha^2 g(x) G^*_m(x) G^*_n(x), G^*_n(x)).$$

Therefore,

$$\gcd((a-b)^2 G'_{m+n+1}(x), G^*_n(x)) = \gcd(\alpha^2 G^*_{m+1}(x) G^*_{n+1}(x), G^*_n(x)).$$

Proposition 2 and $\gcd(\alpha, G_{n+1}) = 1$ imply that $\gcd(\alpha^2 G^*_{n+1}(x), G^*_n(x)) = 1$. Therefore, by Proposition 1 part (2) we have

$$\gcd(G^*_{m+1}(x) G^*_{n+1}(x), G^*_n(x)) = \gcd(G^*_{m+1}(x), G^*_n(x)).$$

This implies that

$$\gcd((a-b)^2 G'_{m+n+1}(x), G^*_n(x)) = \gcd(G^*_{m+1}(x), G^*_n(x)).$$

This and $\gcd((a-b)^2, G^*_n(x)) = 1$ imply that

$$\gcd(G'_{m+n+1}(x), G^*_n(x)) = \gcd(G^*_{m+1}(x), G^*_n(x)).$$

Proof of part (2). From Lemma 1 part (3) it is easy to see that

$$\gcd(G'_{m-n+1}(x), G^*_n(x)) = \gcd((g(x))^n G'_{m+1-n}(x), G^*_n(x)).$$

This and Proposition 3 part (2) (after interchanging the roles of m and n) imply that $\gcd(G'_{m-n+1}(x), G^*_n(x))$ is equal to

$$\gcd(\alpha G'_{m+1}(x) G^*_n(x) - G'_{m+1+n}(x), G^*_n(x)) = \gcd(G'_{m+n+1}(x), G^*_n(x)).$$

The conclusion follows from part (1).

Proof of part (3). From Lemma 1 part (3) it is easy to see that

$$\gcd(G'_{n-m+1}(x), G^*_n(x)) = \gcd((-g(x))^{m-1}G'_{n-(m-1)}(x), G^*_n(x)).$$

This and Proposition 3 part (3) imply that $\gcd(G'_{m-n+1}(x), G^*_n(x))$ is equal to

$$\gcd(G'_{n+m-1}(x) - \alpha G'_{m-1}(x)G^*_n(x), G^*_n(x)) = \gcd(G'_{n+(m-2)+1}(x), G^*_n(x)).$$

The conclusion follows from part (1). □

Theorem 2. *Let $G^*_n(x)$ and $G'_n(x)$ be equivalent GFPs. If m and n are positive integers and $\gcd(m, n) = d$, then*

$$\gcd(G'_m(x), G^*_n(x)) = \begin{cases} G^*_d(x), & \text{if } E_2(m) > E_2(n); \\ \gcd(G^*_d(x), G^*_0(x)), & \text{otherwise.} \end{cases}$$

Proof. Suppose that $E_2(m) > E_2(n)$. We prove this part using cases.

`Case` $m > n$. Since $m > n$, there is a positive integer l such that $m = n + l$. Therefore, $\gcd(G'_m(x), G^*_n(x)) = \gcd(G'_{l-1+n+1}(x), G^*_n(x))$. This and Proposition 10 part (1) imply that $\gcd(G'_m(x), G^*_n(x)) = \gcd(G^*_l(x), G^*_n(x))$. Since $E_2(m) > E_2(n)$ and $m = n + l$, we have $E_2(l) = E_2(n)$. This and Theorem 1 imply that $\gcd(G^*_l(x), G^*_n(x)) = G^*_{\gcd(l,n)}(x)$. From Lemma 3 it is easy to see that $\gcd(l, n) = \gcd(m, n)$. Thus, $\gcd(G^*_l(x), G^*_n(x)) = G^*_{\gcd(m,n)}(x)$. Therefore, we have $\gcd(G'_m(x), G^*_n(x)) = G^*_{\gcd(m,n)}(x)$.

`Case` $m < n$. The proof of this case is similar to the proof of Case $m > n$. It is enough to replace m by $n - (l + 1)$ in $\gcd(G'_m(x), G^*_n(x))$, and then use Proposition 10 part (3).

We now suppose that $E_2(m) \le E_2(n)$. Again we argue using cases.

`Case` $m > n$. So, there is a positive integer l such that $m = l + n$. Therefore, by Proposition 10 part (1) we have

$$\gcd(G'_m(x), G^*_n(x)) = \gcd(G'_{n+(l-1)+1}(x), G^*_n(x)) = \gcd(G^*_l(x), G^*_n(x)).$$

Note that if $m = n + l$ and $E_2(m) \le E_2(n)$, then there are integers k_1, k_2, q_1, and q_2 with $k_1 \le k_2$ such that $m = 2^{k_1}q_1$ and $n = 2^{k_2}q_2$. Since $m = n + l$, we see that $E_2(l) \ne E_2(n)$. This and Theorem 1 imply that

$$\gcd(G^*_l(x), G^*_n(x)) = \gcd(G^*_0(x), G^*_{\gcd(n,l)}(x)).$$

Thus,

$$\gcd(G'_m(x), G^*_n(x)) = \gcd(G^*_0(x), G^*_{\gcd(m,n)}(x)).$$

`Case` $m < n$. The proof of this case is similar to the proof of Case $m > n$. It is enough to replace m by $n - (l + 1) + 1$ in $\gcd(G'_m(x), G^*_n(x))$, and then use Proposition 10 part (3).

`Case` $m = n$. Since $n = (2n-1) - n + 1$, taking $m = 2n - 1$ in Proposition 10 part (2) and using Theorem 1 we obtain that $\gcd(G'_n(x), G^*_n(x))$ is equal to

$$\gcd(G'_{(2n-1)-n+1}(x), G^*_n(x)) = \gcd(G^*_{2n}(x), G^*_n(x)) = \gcd(G^*_0(x), G^*_n(x)).$$

This completes the proof. □

In [11, Theorem 3.4] it is proved that Fibonacci polynomials, Chebyshev polynomials of second kind, Morgan-Voyce polynomials, and Schechter polynomials satisfy the strong divisibility property. In [12, Theorem 7] it is proved that GFP's of Fibonacci type satisfy the strong divisibility property. Theorem 3 proves a necessary and sufficient condition for the polynomials in a generalized Fibonacci polynomial sequence to satisfy the strong divisibility property. Norfleet [22] also proved the same strong divisibility property for GFPs of Fibonacci type.

Theorem 3. *Let $\{G_k(x)\}$ be a GFP sequence that is either Fibonacci type or Lucas type. For any two positive integers m and n it holds that $\{G_k(x)\}$ is a sequence of GFPs of Fibonacci type if and only if* $\gcd(G_m(x), G_n(x)) = G_{\gcd(m,n)}(x)$.

Proof. Let $\{G'_n(x)\}$ be a GFP sequence of Fibonacci type. We now show that $\gcd(G'_m(x), G'_n(x))$ divides $G'_{\gcd(m,n)}(x)$ for $m > 0$, $n > 0$, and vice versa.

If $G'_n(x)$ is of Fibonacci type, by Proposition 6 it is clear that

$$G'_{\gcd(m,n)}(x) \mid \gcd(G'_m(x), G'_n(x)).$$

Next we show that $\gcd(G'_m(x), G'_n(x))$ divides $G'_{\gcd(m,n)}(x)$.

Let $k = \gcd(m, n)$ and assume without the loss of generality that $k \neq n$ and $k \neq m$. The Bézout identity implies that there are two positive integers r and s such that $k = rm - sn$. So, $rm = k + sn$ and $G'_{rm}(x) = G'_{k+sn}(x)$. This, Proposition 3 part (1), and the fact that $k + sn = (k + (sn - 1)) + 1$ imply that

$$G'_{rm}(x) = G'_{k+1}(x)G'_{s'n}(x) + g(x)G'_k(x)G'_{sn-1}(x).$$

We note that by Proposition 6, $G'_m(x) \mid G'_{rm}(x)$ and $G'_n(x) \mid G'_{sn}(x)$. Since both $\gcd(G'_m(x), G'_n(x)) \mid G'_m(x)$ and $\gcd(G'_m(x), G'_n(x)) \mid G'_n(x)$ hold and also both $G'_m(x) \mid G'_{rm}(x)$ and $G'_n(x) \mid G'_{s'n}(x)$ hold, we have that $\gcd(G'_m(x), G'_n(x))$ divides both $G'_{rm}(x)$ and $G'_{s'n}(x)$. This together with Lemma 1 part (3) and the fact that $\gcd(G'_m(x), G'_n(x))$ does not divide $G'_{s'n-1}(x)$ imply that $\gcd(G'_m(x), G'_n(x))$ divides $G'_k(x)$.

Conversely, suppose that $\{G_n(x)\}$ is a GFP sequence such that the strong divisibility property holds or $\gcd(G_m(x), G_n(x)) = G_{\gcd(m,n)}(x)$ for any two positive integers m and n. We now show that both $G_m(x)$ and $G_n(x)$ are GFPs of the Fibonacci type. We prove this using the method of contradiction.

If $G_m(x)$ and $G_n(x)$ are in $\{G_n(x)\}$ such that they are both GFPs of the Lucas type, then by Theorem 1 we obtain a contradiction. This completes the proof. □

6. The gcd Properties of Familiar GFPs and Questions

In this section we formulate a general question and present three tables which are corollaries of the main results in Section 5. These tables give us the strong divisibility property of the familiar polynomials which satisfy the Binet formulas (4) and (6). Table 3 gives the greatest common divisors for Fibonacci polynomials, Pell polynomials, Fermat polynomials, Jacobsthal polynomials, Chebyshev polynomials of the second kind, and one type of Morgan-Voyce (B_n) polynomials. Table 4 gives the strong divisibility property of the Lucas polynomials, Pell-Lucas polynomials, Fermat-Lucas polynomials, Jacobsthal-Lucas polynomials, Chebyshev polynomials of the first kind, and Morgan-Voyce (C_n) polynomials. Table 5 gives the gcd of a polynomial of Lucas type and its equivalent polynomial of Fibonacci type.

We note here that in the case of Table 4, the strong divisibility property is partially satisfied since it only holds when the largest power of 2 that divides m and the largest power of 2 that divides n are equal (that is, $E_2(m) = E_2(n)$). Similarly, the strong divisibility property only holds in Table 5 when $E_2(n) < E_2(m)$.

For simplicity we present the polynomials in Tables 3, 4 and 5 without the variable x.

Polynomial	The Fibonacci gcd property
Fibonacci	$\gcd(F_m, F_n) = F_{\gcd(m,n)}$
Pell	$\gcd(P_m, P_n) = P_{\gcd(m,n)}$
Fermat	$\gcd(\Phi_m, \Phi_n) = \Phi_{\gcd(m,n)}$
Chebyshev the second kind	$\gcd(U_m, U_n) = U_{\gcd(m,n)}$
Jacobsthal	$\gcd(J_m, J_n) = J_{\gcd(m,n)}$
Morgan-Voyce	$\gcd(B_m, B_n) = B_{\gcd(m,n)}$

Table 3: Strong divisibility property of polynomials of Fibonacci type.

Polynomial	Case 1: $E_2(m) = E_2(n)$	Case 2: $E_2(m) \neq E_2(n)$
Lucas	$\gcd(D_m, D_n) = D_{\gcd(m,n)}$	$\gcd(D_m, D_n) = 1$
Pell-Lucas-prime	$\gcd(Q'_m, Q'_n) = Q'_{\gcd(m,n)}$	$\gcd(Q'_m, Q'_n) = 1$
Fermat-Lucas	$\gcd(\vartheta_m, \vartheta_n) = \vartheta_{\gcd(m,n)}$	$\gcd(\vartheta_m, \vartheta_n) = 1$
Chebyshev the first kind	$\gcd(T_m, T_n) = T_{\gcd(m,n)}$	$\gcd(T_m, T_n) = 1$
Jacobsthal-Lucas	$\gcd(Q_m, Q_n) = Q_{\gcd(m,n)}$	$\gcd(Q_m, Q_n) = 1$
Morgan-Voyce	$\gcd(C_m, C_n) = C_{\gcd(m,n)}$	$\gcd(C_m, C_n) = 1$

Table 4: Strong divisibility property (partially) of polynomials of Lucas type.

Polynomials	$E_2(n) < E_2(m)$	Otherwise
Fibonacci, Lucas	$\gcd(F_m, D_n) = D_d$	$\gcd(F_m, D_n) = 1$
Pell, Pell-Lucas-prime	$\gcd(P_m, Q_n^{'}) = Q_d^{'}$	$\gcd(P_m, Q_n^{'}) = 1$
Fermat, Fermat-Lucas	$\gcd(\Phi_m, \vartheta_n) = \vartheta_d$	$\gcd(\Phi_m, \vartheta_n) = 1$
Chebyshev both kinds	$\gcd(U_m, T_n) = T_d$	$\gcd(U_m, T_n) = 1$
Jacobstal, Jacobsthal-Lucas	$\gcd(J_m, j_n,) = j_d$	$\gcd(J_m, j_n) = 1$
Morgan-Voyce both types	$\gcd(B_m, C_n) = C_d$	$\gcd(B_m, C_n) = 1$

Table 5: Strong divisibility property (partially) of polynomials of Lucas type and their equivalents, where $d = \gcd(m, n)$.

6.1. Questions

1. Let $\{G_n^*(x)\}$ and $\{S_n(x)\}$ be generalized Fibonacci polynomial sequences of Lucas type and Fibonacci type, respectively. If $S_n(x)$ is not the equivalent of $G_n^*(x)$, what is the $\gcd(G_k^*(x), S_m(x))$? We believe that the answer is: 1 or x.

2. If $\{G_n(x)\}$ and $\{S_n(x)\}$ are two different generalized Fibonacci polynomial sequences of the same type, then do they satisfy the strong divisibility property?

3. (**Conjecture.**) The GFPs T_n and S_m satisfy the strong divisibility property if and only if T_n and S_m are both of Fibonacci type and they belong to the same generalized Fibonacci polynomial sequence. Theorems 2, 3, and [3, Lemma 4] suggest that the conjecture is true.

4. Let $\mathcal{R}$ be a set of recursive functions. If $\mathcal{F} : \mathbb{N} \to \mathcal{R}$, $\mathcal{G} : \mathcal{R} \times \mathcal{R} \to \mathcal{R}$, and $g : \mathbb{N} \times \mathbb{N} \to \mathbb{N}$. Under what conditions $\mathcal{G} \circ (\mathcal{F} \times \mathcal{F}) = \mathcal{F} \circ g$ for all $\mathcal{F} \in \mathcal{R}$ and a fixed g?

Acknowledgement. We would like to thank an anonymous referee for suggesting that we refer to papers [3, 23] which helped us improve the paper.

References

[1] R. André-Jeannin, Differential properties of a general class of polynomials, *Fibonacci Quart.* **33** (1995), 453–458.

[2] S. Barbero, Generalized Vandermonde determinants and characterization of divisibility sequences, J. Number Theory **173** (2017), 371–377.

[3] N. Bliss, B. Fulan, S. Lovett, and J. Sommars, Strong divisibility, cyclotomic polynomials, and iterated polynomials, *Amer. Math. Monthly* **120** (2013), 519–536.

[4] R. Flórez, R. Higuita, and A. Mukherjee, Alternating sums in the Hosoya polynomial triangle, *J. Integer Seq.* **17** (2014), Article 14.9.5.

[5] R. Flórez, R. Higuita, and L. Junes, 9-modularity and gcd properties of generalized Fibonacci numbers, *Integers* **14** (2014), Paper No. A55.

[6] R. Flórez and L. Junes, gcd properties in Hosoya's triangle, *Fibonacci Quart.* **50** (2012), 163–174.

[7] R. Flórez, N. McAnally, and A. Mukherjee, Identities for the generalized Fibonacci polynomial, submitted. `https://arxiv.org/abs/1702.01855`

[8] M. Hall, Divisibility sequences of third order, *Amer. J. Math.* **58** (1936), 577–584.

[9] R. T. Hansen, Generating identities for Fibonacci and Lucas triples, *Fibonacci Quart.* **10** (1972), 571–578.

[10] P. Hilton, P. J. Pedersen, and L. Vrancken, On certain arithmetic properties of Fibonacci and Lucas numbers, *Fibonacci Quart.* **3** (1995), 211–217.

[11] V. E. Hoggatt, Jr., and M. Bicknell-Johnson, Divisibility properties of polynomials in Pascal's triangle, *Fibonacci Quart.* **16** (1978), 501–513.

[12] V. E. Hoggatt, Jr., and C. T. Long, Divisibility properties of generalized Fibonacci polynomials, *Fibonacci Quart.* **12** (1974), 113–120.

[13] A. F. Horadam, A synthesis of certain polynomial sequences, *Applications of Fibonacci numbers*, Vol. 6 (Pullman, WA, 1994), 215–229, Kluwer Acad. Publ., Dordrecht, 1996.

[14] A. F. Horadam and J. M. Mahon, Pell and Pell-Lucas polynomials, *Fibonacci Quart.* **23** (1985), 7–20.

[15] A. F. Horadam, Chebyshev and Fermat polynomials for diagonal functions, *Fibonacci Quart.* **17** (1979), 328–333.

[16] C. Kimberling, Greatest common divisors of sums and differences of Fibonacci, Lucas, and Chebyshev polynomials, *Fibonacci Quart.* **17** (1979), 18–22.

[17] C. Kimberling, Strong divisibility sequences and some conjectures, *Fibonacci Quart.* **17** (1979), 13–17.

[18] C. Kimberling, Strong divisibility sequences with nonzero initial term, *Fibonacci Quart.* **16** (1978), 541–544.

[19] T. Koshy, *Fibonacci and Lucas Numbers with Applications*, John Wiley, New York, 2001.

[20] E. Lucas, Théorie des fonctions numériques simplement périodiques, *Amer. J. Math.* **1** (1878), 184–240, 289–321.

[21] W. McDaniel, The g.c.d. in Lucas sequences and Lehmer number sequences, *Fibonacci Quart.* **29** (1991), 24–29.

[22] M. Norfleet, Characterization of second-order strong divisibility sequences of polynomials, *Fibonacci Quart.* **43** (2005), 166–169.

[23] A. Nowicki, Strong divisibility and LCM-sequences, *Amer. Math. Monthly* **122** (2015), 958–966.

[24] M. O. Rayes, V. Trevisan, and P. S. Wang, Factorization properties of Chebyshev polynomials, *Comput. Math. Appl.* **50** (2005), 1231–1240.

[25] M. Ward, Note on divisibility sequences, *Bull. Amer. Math. Soc.* **42** (1936), 843–845.

[26] W. A. Webb and E. A. Parberry, Divisibility properties of Fibonacci polynomials, *Fibonacci Quart.* **7** (1969), 457–463.