ON THE DISCRIMINANT OF THE k-GENERALIZED FIBONACCI POLYNOMIAL

FLORIAN LUCA

Abstract. In this paper, we make some remarks about the discriminant of the k-generalized Fibonacci polynomial $X^k - X^{k-1} - \cdots - X - 1$ and use our results to confirm a conjecture of Hashemi and Pirzadeh concerning the period of a sequence related to the k-generalized Fibonacci sequence.

1. Introduction

Let $k \geq 2$ be an integer. Let $f_k(X) := X^k - X^{k-1} - \cdots - X - 1$. This is sometimes called the k-generalized Fibonacci polynomial because it is the characteristic polynomial of the sequence of k-generalized Fibonacci numbers $\{F_n^{(k)}\}_{n \geq 0}$ given by $F_0^{(k)} = \cdots = F_{k-2}^{(k)} = 0$, $F_{k-1}^{(k)} = 1$. We label the roots as $\alpha_1, \ldots, \alpha_k$. It is known that $f_k(X)$ has only one positive real root, let us call it α_1. This root satisfies $\alpha_1 > 1$. Furthermore, $|\alpha_i| < 1$ for $i = 2, \ldots, k$. If k is odd, then α_i are complex and nonreal for all $i = 2, \ldots, k$, whereas when k is even, $f_k(X)$ has an additional real root, let us call it α_2, and it is in the interval $(-1, 0)$. Because all algebraic conjugates of α_1 are inside the unit disk, it follows that α_1 is a *Pisot number* and, in particular, $f_k(X)$ is irreducible in $\mathbb{Q}[X]$.

In this note, we look at the polynomials

$$g_k(X) := \prod_{i=1}^{k} (X - \alpha_i^2); \quad \text{and} \quad h_k(X) := \prod_{1 \leq i < j \leq k} (X - \alpha_i \alpha_j).$$

We prove some results about their discriminants, make some conjectures, and answer in the affirmative a conjecture from [3]. Table 1 gives their discriminants for $k \in \{3, 4, \ldots, 10\}$.

k	$\mathrm{Disc}(f_k)$	$\mathrm{Disc}(g_k)$	$\mathrm{Disc}(h_k)$
3	$-2^2 \times 11$	$-2^4 \times 11$	$-2^2 \times 11$
4	-563	-563	$2^2 \times 563^2$
5	$2^4 \times 599$	$2^8 \times 599$	$2^{20} \times 599^3$
6	205937	205937	$2^{18} \times 205937^4$
7	$-2^6 \times 84223$	$-2^{12} \times 84223$	$-2^{66} \times 84223^5$
8	-1319×126913	-1319×126913	$2^{60} \times 1319^6 \times 126913^6$
9	$2^8 \times 17 \times 487 \times 2851$	$2^{16} \times 17 \times 487 \times 2851$	$2^{152} \times 17^7 \times 487^7 \times 2851^7$
10	7×35616734267	7×35616734267	$2^{140} \times 7^8 \times 35616734267^8$

Table 1: Discriminants of f_k, g_k, and h_k for $k = 3, 4, \ldots 10$.

We use the letter t to denote one of the polynomials f, g, h. For $F(X) \in \mathbb{Z}[X]$ we use $\mathrm{Disc}(F(X))$ for its discriminant. We write

$$\mathrm{Disc}(t_k) := (-1)^{s_{t_k}} 2^{a_{t_k}} b_{t_k}, \quad s_{t_k} \in \{0, 1\},\ a_{t_k} \in \mathbb{Z},\ b_{t_k} \equiv 1 \pmod 2,\ b_{t_k} \geq 1, \quad t \in \{f, g, h\}.$$

This work was done when the author visited the Max Planck Institutes for Mathematics (Bonn, Spring 2019) and Software Systems (Saarbrücken, 2020). In addition, the author was supported by grant RTNUM19 from CoEMaSS, Wits, South Africa.

Thus, $(-1)^{s_k}$ denotes the sign, a_{t_k} denotes the exponent of 2 in the factorization, and $b_{t_k} \geq 1$ denotes the largest odd factor of $\mathrm{Disc}(t_k)$, respectively, for $t \in \{f, g, h\}$. Our goal is to give formulas for s_{t_k}, a_{t_k}, and b_{t_k} for $t \in \{f, g, h\}$. These formulas are inspired by the entries in Table 1. Let $\nu_p(m)$ be the exponent of p in the factorization of the positive integer m.

Theorem 1.1. *Let $k \geq 3$. The following hold:*

(i)
$$s_{f_k} = s_{g_k} \equiv \frac{(k-1)(k+2)}{2} \pmod 2 = \begin{cases} 0, & \text{if } k \equiv 1, 2 \pmod 4; \\ 1, & \text{if } k \equiv 0, 3 \pmod 4. \end{cases}$$

Further,
$$s_{h_k} \equiv \left\lfloor \frac{k-1}{2} \right\rfloor (k-2) \pmod 2 = \begin{cases} 0, & \text{if } k \equiv 0, 1, 2 \pmod 4; \\ 1, & \text{if } k \equiv 3 \pmod 4. \end{cases}$$

(ii)
$$b_{f_k} = b_{g_k} = \frac{2^{k+1}k^k - (k+1)^{k+1}}{2^{a_{f_k}}(k-1)^2}, \quad \text{and} \quad b_{h_k} = (b_{f_k})^{k-2}.$$

(iii)
$$a_{f_k} = \begin{cases} 0, & \text{if } k \equiv 0 \pmod 2; \\ k-1, & \text{if } k \equiv 1 \pmod 2, \end{cases} \quad \text{and} \quad a_{g_k} = 2a_{f_k}.$$

We did not succeed in finding a_{h_k}. Computations suggest the following pattern.

Conjecture 1.2. *We have*
$$a_{h_k} = \begin{cases} \frac{k(k-2)(k-3)}{2}, & \text{if } k \equiv 0 \pmod 2; \\ \frac{(k-1)(k^2-5)}{4}, & \text{if } k \equiv 1 \pmod 2. \end{cases}$$

We leave the above conjecture as an open problem for the reader.

In [3], the authors introduced the following doubly indexed sequence $g_n^{(k)}$ for $k \geq 3$ and $n \geq 0$:
$$\begin{aligned}
&g_0^{(3)} = g_1^{(3)} = g_2^{(3)} = g_3^{(3)} = 0, \quad g_4^{(3)} = 1, \quad g_5^{(3)} = 6, \\
&g_n^{(3)} = g_{n-1}^{(3)} + g_{n-2}^{(3)} + g_{n-2}^{(3)} + F_{n-3}^{(3)}(F_{n-1}^{(3)} - F_{n-2}^{(3)}) + (F_{n-3}^{(3)} + F_{n-2}^{(3)})(F_n^{(3)} - F_{n-1}^{(3)}), \quad n \geq 3; \\
&g_0^{(k)} = g_1^{(k)} = g_2^{(k)} = 0, \quad g_3^{(k)} = g_3^{(k-1)}, \quad \ldots, \quad q_{k+1}^{(k)} = g_{k+1}^{(k-1)}, \quad \text{for} \quad k \geq 4; \\
&g_n^{(k)} = g_{n-1}^{(k)} + \cdots + g_{n-k}^{(k)} + F_{n-3}^{(k)}(F_{n-1}^{(k)} - F_{n-2}^{(k)}) + (F_{n-3}^{(k)} + F_{n-2}^{(k)})(F_n^{(k)} - F_{n-1}^{(k)}) \\
&\qquad + (F_{n-3}^{(k)} + F_{n-2}^{(k)} + F_{n-1}^{(k)})(F_{n+1}^{(k)} - F_n^{(k)}) + \cdots \\
&\qquad + (F_{n-3}^{(k)} + \cdots + F_{n+k-5}^{(k)})(F_{n+k-3}^{(k)} - F_{n+k-4}^{(k)}), \quad n \geq k+2, \quad \text{and} \quad k \geq 4.
\end{aligned}$$

The above sequence arose naturally in the context of a k-Fibonacci sequence of elements in a certain nilpotent group. Namely, consider an integer $m \geq 2$, and the group
$$G_m := \langle x, y \mid x^m = y^m = 1; [x, y]^x = [x, y]^y = [x, y] \rangle.$$

As usual, for elements g, h of a group G we use the commutator notation $[g, h] := g^{-1}h^{-1}gh$ and g^h is the conjugation of g by h given by $g^h := h^{-1}gh$. It turns out that G_m is a group of order m^3, with $G' = Z(G) = \langle [y, x] \rangle$, and
$$\frac{G}{G'} \cong \frac{\mathbb{Z}}{m\mathbb{Z}} \oplus \frac{\mathbb{Z}}{m\mathbb{Z}}.$$

Further, every element of G_m is representable in a unique way as $x^a y^b [y,x]^c$ for some integers $a,b,c \in \{0,1,\ldots,m-1\}$. For $k \geq 3$, let $\{x_n^{(k)}\}_{n\geq 1} \subset G$ be given by $x_1 = x$, $x_2 = y$, $x_n = x_1 \cdots x_{n-1}$ for $3 \leq n \leq k$, and $x_n = x_{n-k} \cdots x_{n-1}$ for $n \geq k+1$. Then the main theorem of [3] shows that for $k \geq 4$, one has

$$x_n^{(k)} = x^{F_{n+k-2}^{(k)} - F_{n+k-3}^{(k)}} y^{F_{n+k-3}^{(k)}} [y,x]^{g_n^{(k)}}$$

for all $n \geq 1$. Because all elements in G_m have order dividing m, only the residue classes of the above exponents of x, y, $[y,x]$ modulo m matter. Letting $K(k,m)$ denote the period of the k-Fibonacci sequence modulo m, the authors of [3] conjectured that the sequence $\{x_n^{(k)}\}_{n\geq 0}$ is periodic modulo m with period $L(k,m)$ that, when $m = p$ is a prime, satisfies

$$L(k,p) = \begin{cases} 2K(k,2), & \text{if } p = 2; \\ K(k,p), & \text{if } p \geq 3. \end{cases} \tag{1.1}$$

Note that, by looking only at the exponent of y, it follows that $K(k,p)$ must divide $L(k,p)$. Thus, what remains is to decide whether the sequence $\{g_n^{(k)}\}_{n\geq 0}$ is periodic modulo p with period $2K(k,2)$ for $p = 2$ and $K(k,p)$ for $p > 2$. In [3], the conjecture was proved for $p = 2$. In this note, we use our Theorem 1.1 to prove that the conjecture is not entirely correct, but an amended version of it is correct. Namely, we have the following result.

Theorem 1.3. *If $p > 2$ is prime, then $\{x_n^{(k)}\}_{n\geq 1}$ is periodic with period $L(k,p) = K(k,p)$ modulo p except when $p \mid k-1$, in which case $L(k,p) = pK(k,p)$.*

2. The Proof of Theorem 1.1

The discriminant of $f_k(X)$ has been computed in many places. One of them is Lemma 2.3 in [4]. Its formula is

$$\mathrm{Disc}(f_k(X)) = (-1)^{\binom{k+1}{2}-1} \left(\frac{2^{k+1}k^k - (k+1)^{k+1}}{(k-1)^2} \right).$$

The exponent of (-1) is $\binom{k+1}{2} - 1 = \dfrac{(k-1)(k+2)}{2}$. Let

$$A_k := \left(\frac{2^{k+1}k^k - (k+1)^{k+1}}{(k-1)^2} \right).$$

It is known that A_k is positive. Let us supply a quick proof of it. We check that $A_2 = 5 > 0$. For $k \geq 3$, the inequality

$$2^{k+1}k^k > (k+1)^{k+1} \quad \text{is equivalent to} \quad 2^{k+1} > (k+1)\left(1 + \frac{1}{k}\right)^k.$$

Because $(1+1/k)^k < e$, it follows that it suffices to show that $2^{k+1} > e(k+1)$. One can prove this by induction on $k \geq 3$ starting with $k = 3$, where $16 > 4e$. This is obvious. We are now ready to discuss $\nu_2(A_k)$. If k is even, then $k+1$ is odd, so $2^{k+1}k^k - (k+1)^{k+1}$ is odd. Thus, $\nu_2(A_k) = 0$ for even k. If $k \equiv 3 \pmod 4$, then $2 \mid k-1$ and $(k+1)/2$ is even. Hence,

$$A_k = 2^{k-1} \left(\frac{k^k - ((k+1)/2)^{k+1}}{((k-1)/2)^2} \right), \tag{2.1}$$

and the cofactor of 2^{k-1} has both its numerator and its denominator odd. It then follows that $k - 1 = \nu_2(A_k)$. For $k \equiv 1 \pmod 4$, the problem is a bit harder. We follow the method from

[2]. Namely, we work with the representation (2.1) of A_k. We calculate the numerator of the cofactor of 2^{k-1} modulo $((k-1)/2)^3$ getting

$$\begin{aligned}
k^k - ((k+1)/2)^{k+1} &= ((k-1)+1)^k - \left(\left(\frac{k-1}{2}\right)+1\right)^{k+1} \\
&\equiv \left(\binom{k}{2}(k-1)^2 + \binom{k}{1}(k-1) + 1\right) \\
&\quad - \left(\binom{k+1}{2}\left(\frac{k-1}{2}\right)^2 + \binom{k+1}{1}\left(\frac{k-1}{2}\right) + 1\right) \mod \left(\frac{k-1}{2}\right)^3 \\
&\equiv \left(\frac{k-1}{2}\right)^2 \left(4\binom{k}{2} - \binom{k+1}{2}\right) + \left(\frac{k-1}{2}\right)(k-1) \mod \left(\frac{k-1}{2}\right)^3 \\
&\equiv \left(\frac{k-1}{2}\right)^2 \left(4\binom{k}{2} - \binom{k+1}{2} + 2\right) \mod \left(\frac{k-1}{2}\right)^3.
\end{aligned}$$

Thus,

$$\begin{aligned}
\frac{k^k - ((k+1)/2)^{k+1}}{((k-1)/2)^2} &\equiv 4\binom{k}{2} - \binom{k+1}{2} + 2 \pmod{(k-1)/2} \\
&\equiv 2k(k-1) - \frac{((k-1)+2)k}{2} + 2 \pmod{(k-1)/2} \\
&\equiv -k + 2 \pmod{(k-1)/2} \\
&\equiv 1 \pmod{(k-1)/2}.
\end{aligned}$$

Thus,

$$\frac{k^k - ((k+1)/2)^{k+1}}{((k-1)/2)^2} \equiv 1 \pmod{(k-1)/2}. \tag{2.2}$$

The above calculation is valid for every odd $k \geq 3$. In particular, for $k \equiv 1 \pmod 4$, we have that $2 \mid (k-1)/2$, so $\nu_2(A_k) = k-1$. A similar calculation can be carried through when k is even. This has been done in [2]. There it was shown that

$$A_k \equiv \frac{k(k-1)^2(7k-17)}{6} 2^{k-2} + k(3k-5)2^{k-2} + 2^k \pmod{(k-1)^2}.$$

Because $k(k-1)(7k-17)/6$ is always an integer, we have

$$A_k \equiv ((k-1)+1)(3(k-1)-2)2^{k-2} + 2^k \equiv 2^{k-1} \pmod{k-1}. \tag{2.3}$$

Let us notice that congruences (2.2) and (2.3) show that $\gcd(k-1, A_k)$ is a power of 2 and because $2^{k-1} \mid A_k$, we get that $\gcd(k-1, A_k) = 2^{\nu_2(k-1)}$. This also implies that $3 \nmid \mathrm{Disc}(f_k)$. Indeed, this is clear if $3 \mid k$, because then 3 divides $2^{k+1}k^k$ but not $(k+1)^{k+1}$. It is also clear if $k \equiv 2 \pmod 3$, because then 3 divides $(k+1)^{k+1}$ but not $2^{k+1}k^k$. Finally, if $k \equiv 1 \pmod 3$, then $3 \mid k-1$ and that $3 \nmid \mathrm{Disc}(f_k)$ now follows from $\gcd(k-1, \mathrm{Disc}(f_k)) = 2^{\nu_2(k-1)}$. Let us summarize what we have proved.

Lemma 2.1. *The following hold:*

$$\mathrm{Disc}(f_k) = (-1)^{(k-1)(k+2)/2} A_k, \quad \text{where} \quad A_k := \frac{2^{k+1}k^k - (k+1)^{k+1}}{(k-1)^2}.$$

Further,

(i) $A_k > 0$;

(ii) $\nu_2(A_k) = 0$, *if* k *is even; and* $\nu_2(A_k) = k-1$, *if* k *is odd;*
(iii) $\gcd(k-1, A_k) = 2^{\nu_2(k-1)}$;
(iv) $3 \nmid A_k$ *for any* $k \geq 2$.

Proof of Theorem 1.1 (i). In Lemma 2.1, we showed that $s_{f_k} \equiv (k-1)(k+2)/2 \pmod 2$. It is also known that s_{f_k} is congruent to $s \pmod 2$, where $2s$ is the number of complex conjugated roots of $f_k(X)$. In our case, $s = \lfloor (k-1)/2 \rfloor$. For $g_k(X)$, we note that its roots are α_i^2 for $i = 1, \ldots, k$. Because $\alpha_1 > 1$ is a Pisot number, it follows that α_1^2 is also a Pisot number, In particular, $g_k(X)$ is irreducible. It has the same number of complex conjugated roots as $f_k(X)$. The only way in which it will have a different number of complex conjugates roots would be if α_i^2 is real for some complex nonreal α_i. This would imply that $\alpha_i^2(\overline{\alpha_i})^{-2} = 1$, which is a nontrivial multiplicative relation among the conjugates of a Pisot number, and is impossible by a result of Mignotte [5]. Finally, for $h_k(X)$, its roots are $\alpha_i\alpha_j$ for $1 \leq i < j \leq k$. They are all distinct again by Mignotte's result. Further, $\alpha_i\alpha_j$ is complex nonreal if either α_i is real and α_j is complex nonreal, or if α_i is complex nonreal and α_j is also complex nonreal and different from α_i and $\overline{\alpha_i}$. Conversely, if α_i is real and α_j is complex nonreal, then $\alpha_i\alpha_j$ is also complex nonreal. Further, if α_i and α_j are complex nonreal and α_j is not the complex conjugate of α_i, then $\alpha_i\alpha_j$ is complex nonreal. If not, we would get that $\alpha_i\alpha_j = \overline{\alpha_i\alpha_j}$, with $\alpha_i \neq \overline{\alpha_j}$, again a nontrivial multiplicative relation that does not exist by Mignotte's result. Thus, the number of complex conjugated roots of h_k is $(k-2s)2s + 2s(2s-2) = 2s(k-2)$, so the number of such complex conjugated pairs is $s(k-2) = \lfloor (k-1)/2 \rfloor (k-2)$, which is what we wanted.

We prove (iii) next. The statement about a_{f_k} follows from Lemma 2.1. For a_{g_k}, we calculate

$$|\mathrm{Disc}(g_k)| = \left(\prod_{1 \leq i < j \leq k} (\alpha_i^2 - \alpha_j^2) \right)^2 = \left(\prod_{1 \leq i < j \leq k} (\alpha_i - \alpha_j) \right)^2 \left(\prod_{1 \leq i < j \leq k} (\alpha_i + \alpha_j) \right)^2$$
$$= A_k \left(\prod_{1 \leq i < j \leq k} (\alpha_i + \alpha_j) \right)^2.$$

To compute the second factor, note that

$$2\alpha_i \prod_{i \neq j} (\alpha_i + \alpha_j) = (-1)^k f_k(-\alpha_i) = \alpha_i^k + \left(\alpha_i^k - \alpha_i^{k-1} + \cdots + (-1)^{k-1} \right)$$
$$= \alpha_i^k + \frac{\alpha_i^k - (-1)^k}{\alpha_i + 1} = \frac{\alpha_i^{k+1} + 2\alpha_i^k - (-1)^k}{1 + \alpha_i} = \begin{cases} \frac{4\alpha_i^k}{1+\alpha_i}, & \text{if } \ k \equiv 1 \pmod 2; \\ \frac{2\alpha^{k+1}}{1+\alpha_i}, & \text{if } \ k \equiv 0 \pmod 2, \end{cases}$$

where we used $0 = (\alpha_i - 1) f_k(\alpha_i) = \alpha_i^{k+1} - 2\alpha_i^k + 1$. Thus,

$$\left| \prod_{1 \leq i < j \leq k} (\alpha_i + \alpha_j)^2 \right| = 2^{\delta_k} \left(\prod_{i=1}^{k} \frac{|\alpha_i^{\gamma_k}|}{|1 + \alpha_i|} \right) = \frac{2^{\delta_k}}{|f_k(-1)|},$$

where $(\delta_k, \gamma_k) := (k, k-1)$, or $(0, k)$ according to whether $k \equiv 1 \pmod 2$, or $k \equiv 0 \pmod 2$, respectively. Because $|f_k(-1)| = 2,\ 1$ for k odd and even, respectively, we get that

$$\left| \prod_{1 \leq i < j \leq k} (\alpha_i + \alpha_j)^2 \right| = \left\{ \begin{matrix} 2^{k-1}, & \text{if } \ k \equiv 1 \pmod 2 \\ 1, & \text{if } \ k \equiv 0 \pmod 2 \end{matrix} \right\} = 2^{a_{f_k}}.$$

This proves that $a_{g_k} = \nu_2(A_k) + a_{f_k} = 2a_{f_k}$, which is (iii) but also that $b_{g_k} = b_{f_k}$, which is the first part of (ii).

We now prove the second part of (ii). For this, we need a lemma.

Lemma 2.2. *Let p be an odd prime such that $f_k(X) \pmod p$ has a double root. Then, the double root is unique, it is not a triple root, and it is not equal to 1.*

Proof. Assume that $f_k(X) \pmod p$ has a double root. Then, $p \mid A_k$. If the double root is 1, then $f_k(1) \equiv 0 \pmod p$. Because $f_k(1) = -(k-1)$, it follows that $p \mid k-1$. However, by Lemma 2.1 (iii), we know that $\gcd(k-1, A_k)$ is a power of 2. Thus, 1 is not a double root. Now let α be a double root of $f_k(X)$ modulo p. Then, α is a double root of $(X-1)f_k(X) = X^{k+1} - 2X^k + 1$. Because it is a double root, we have that α is a root of the derivative $(k+1)X^k - 2kX^{k-1}$. Clearly, $\alpha \neq 0$. Thus, $(k+1)\alpha \equiv 2k \pmod p$. It follows that p cannot divide $k+1$ (otherwise it would divide $2k$, so k and $k+1$, which is false), so $\alpha \equiv 2k(k+1)^{-1} \pmod p$. This shows that α is unique. If α were a triple root of $f_k(X)$, then α would also be a root of the second derivative $k(k+1)X^{k-1} - 2k(k-1)X^{k-2} \pmod p$ of $(X-1)f_k(X)$. Thus, $k(k+1)\alpha \equiv 2k(k-1) \pmod p$. Clearly, p cannot divide k, otherwise $\alpha \equiv 0 \pmod p$, which is not the case. Hence, $\alpha \equiv 2(k-1)(k+1)^{-1} \pmod p$. Hence, we get that $2k(k+1)^{-1} \equiv 2(k-1)(k+1)^{-1} \pmod p$, so $k \equiv k-1 \pmod p$, which is a contradiction. □

We are now ready to deal with b_{h_k}. Let p be an odd prime such that $p \mid \mathrm{Disc}(h_k(X))$. This means that there exist $i < j,\ r < s$ in $\{1, \ldots, k\}$ with $(i, j) \neq (r, s)$ such that $\alpha_i\alpha_j \equiv \alpha_r\alpha_s \pmod p$. For this part of the proof, we work in an extension of $\mathbb{F}_p$ that contains all the roots of $f_k(X)$. Each $\alpha \in \{\alpha_i, \alpha_j, \alpha_r, \alpha_s\}$ satisfies $\alpha^{k+1} - 2\alpha^k + 1 \equiv 0 \pmod p$, which can be rewritten as $\alpha - 2 \equiv -\alpha^{-k} \pmod p$. We multiply the above two relations for $\alpha \in \{\alpha_i, \alpha_j\}$ to get $(\alpha_i - 2)(\alpha_j - 2) \equiv (\alpha_i\alpha_j)^{-k} \pmod p$. Thus, $\alpha_i\alpha_j - 2(\alpha_i + \alpha_j) + 4 \equiv (\alpha_i\alpha_j)^{-k} \pmod p$. We write down the analogous relation for (i, j) replaced by (r, s) and subtract them using $\alpha_i\alpha_j - \alpha_r\alpha_s \equiv 0 \pmod p$, to get $2(\alpha_i + \alpha_j - \alpha_r + \alpha_s) \equiv 0 \pmod p$. This gives $\alpha_i + \alpha_j \equiv \alpha_r + \alpha_s \pmod p$. Writing $S := \alpha_i + \alpha_j$ and $P := \alpha_i\alpha_j$, we get that both pairs (α_i, α_j) and (α_r, α_s) are the roots of $x^2 - Px + S \equiv 0 \pmod p$. Because a quadratic equation with roots in a field has exactly two solutions (counted with multiplicity), we get $\{\alpha_i, \alpha_j\} \equiv \{\alpha_r, \alpha_s\} \pmod p$. This shows that $f_k(X)$ has multiple roots modulo p. Thus, $p \mid A_k$. Next, from Lemma 2.2, we know that for such p, $f_k(X)$ has exactly one double root that is not a triple root. So, the equality $\{\alpha_i, \alpha_j\} \equiv \{\alpha_r, \alpha_s\} \pmod p$ is only possible with $(i, j) \neq (r, s)$ if $i = j$ and $\alpha_r \equiv \alpha_s \pmod p$ is the only double root of $f_k(X)$ modulo p, or vice versa $j = s$ and $\alpha_i \equiv \alpha_r \pmod p$ is the only double root of $f_k(X)$ modulo p. This shows that the odd part of $\mathrm{Disc}(h_k(X))$ is the largest odd factor of

$$\left| \prod_{\substack{1 \le i < j \le k \\ r \notin \{i,j\}}} (\alpha_i\alpha_r - \alpha_j\alpha_r)^2 \right| = \left| \prod_{r=1}^{k} \alpha_r^2 \right|^{\binom{k-2}{2}} \left| \prod_{1 \le i < j \le k} (\alpha_i - \alpha_j)^2 \right|^{k-2} = A_k^{k-2} = 2^{a_{f_k}(k-2)} b_{f_k}^{k-2}.$$

This shows that $b_{h_k} = b_{f_k}^{k-2}$. It also shows that

$$\prod_{\substack{1 \le i < j \le k \\ 1 \le r < s \le k \\ \#\{i,j,r,s\} = 4}} (\alpha_i\alpha_j - \alpha_r\alpha_s)^2$$

is a power of 2 (note that it is an integer because it is a symmetric polynomial with integer coefficients in all the $\alpha_1, \ldots, \alpha_k$). We leave it to the reader to compute it and confirm Conjecture 1.2.

Remark. It is likely that $h_k(X)$ is irreducible as a polynomial in $\mathbb{Z}[X]$. This is clearly so if k is even or an odd prime by the main result from [4] that asserts that the Galois group of $f_k(X)$ over $\mathbb{Q}$ is the full symmetric group S_k for such values of k. In particular, this Galois group is two transitive showing that all $\alpha_i\alpha_j$ for $i < j$ are Galois conjugated. We do not know how to prove that $h_k(X) \in \mathbb{Z}[X]$ is irreducible for the other values of k, namely the odd composite ones.

3. The Proof of Theorem 1.3

Because the sequence

$$g_n^{(k)} = g_{n-1}^{(k)} + \cdots + g_{n-k}^{(k)} + w_n^{(k)} \quad \text{for all} \quad n \geq k+2,$$

where

$$w_n^{(k)} = \sum_{j=0}^{k-2} \left(\sum_{i=0}^{j} F_{n-3+i}^{(k)} \right) \left(F_{n-1+j}^{(k)} - F_{n-2+j}^{(k)} \right) \quad \text{for all} \quad n \geq k+2,$$

and $\{w_n^{(k)}\}_{n\geq 0}$ is linearly recurrent with simple roots in the set

$$\{\alpha_i^2 : 1 \leq i \leq k\} \cup \{\alpha_i\alpha_j : 1 \leq i < j \leq k\},$$

it follows that $\{g_n^{(k)}\}_{n\geq 0}$ is linearly recurrent with simple roots in the set

$$\{\alpha_i : 1 \leq i \leq k\} \cup \{\alpha_i^2 : 1 \leq i \leq k\} \cup \{\alpha_i\alpha_j : 1 \leq i < j \leq k\}.$$

Thus, a characteristic polynomial for $\{g_n^{(k)}\}_{n\geq 0}$ is $F_k(X) := f_k(X)g_k(X)h_k(X)$. To understand the period modulo p, we need to understand whether $F_k(X)$ has double roots or not modulo p. But if p is an odd prime dividing $\mathrm{Disc}(F_k(X))$, then p divides one of the discriminants $\mathrm{Disc}(f_k)$, $\mathrm{Disc}(g_k)$, $\mathrm{Disc}(h_k)$ (so, $p \mid A_k$ by Theorem 1.1), or p divides one of the resultants

$$\mathrm{Res}(f_k(X), g_k(X)), \quad \mathrm{Res}(f_k(X), h_k(X)), \quad \mathrm{Res}(g_k(X), h_k(X)).$$

In this last case, we show that p divides A_k, or p divides $k-1 = f_k(1)$. Assume $p \mid \mathrm{Res}(f_k(X), h_k(X))$. This last number is, up to sign,

$$\prod_{1\leq i<j\leq k} f_k(\alpha_i\alpha_j).$$

We have

$$\begin{aligned}
(\alpha_i\alpha_j - 1)f_k(\alpha_i\alpha_j) &= (\alpha_i\alpha_j)^{k+1} - 2(\alpha_i\alpha_j)^k + 1 \\
&= (2\alpha_i^k - 1)(2\alpha_j^k - 1) - 2(\alpha_i\alpha_j)^k + 1 = 2((\alpha_i\alpha_j)^k - \alpha_i^k - \alpha_j^k + 1) \\
&= 2(\alpha_i^k - 1)(\alpha_j^k - 1) = 2(\alpha_i\alpha_j)^k(\alpha_i - 1)(\alpha_j - 1). \qquad (3.1)
\end{aligned}$$

Further, the algebraic integers $\alpha_i - 1$ and $\alpha_i\alpha_j - 1$ do not have odd prime ideals in common (prime ideals sitting above odd prime p from $\mathbb{Z}$) because if $\pi \mid p$ would divide $\alpha_i - 1$ and $\alpha_i\alpha_j - 1$ for some prime ideal in $\mathcal{O}_{\mathbb{K}}$, where $\mathbb{K} := \mathbb{Q}(\alpha_1, \ldots, \alpha_k)$, then $\pi \mid (\alpha_i - 1)\alpha_j + (\alpha_j - 1)$, so also $\pi \mid \alpha_j - 1$, therefore $\pi \mid \alpha_i - \alpha_j$, which implies that $\pi \mid A_k$. However, π also divides

$\alpha_i - 1$, which divides $f_k(1) = k - 1$, so π divides $\gcd(k-1, A_k)$, and this is not possible by Lemma 2.1 (iii). This shows that the integer

$$\mathrm{Res}(f_k, h_k) = \prod_{1 \le i < j \le k} f_k(\alpha_i \alpha_j),$$

and the integer

$$\prod_{1 \le i < j \le k} (\alpha_i - 1)(\alpha_j - 1) = \prod_{i=1}^{k} (\alpha_i - 1)^{k-1} = (k-1)^{k-1}$$

have the same largest odd factor. In particular, any odd prime p dividing $\mathrm{Res}(f_k(X), h_k(X))$ divides $k - 1$. Similarly, calculation (3.1) is valid when $i = j$ also, which gives

$$(\alpha_i^2 - 1) f_k(\alpha_i^2) = 2\alpha_i^{2k} (\alpha_i - 1)^2, \quad \text{therefore} \quad f(\alpha_i^2) = \left(\frac{2\alpha_i^{2k}}{1 + \alpha_i} \right) (\alpha_i - 1).$$

This shows that

$$\left| \prod_{i=1}^{k} f_k(\alpha_i^2) \right| = \left| \prod_{i=1}^{k} \left(\frac{2\alpha_i^{2k}}{1 + \alpha_i} \right) (\alpha_i - 1) \right| = 2^{k-1}(k-1).$$

Thus, if p is odd and $p \mid \mathrm{Res}(f_k(X), g_k(X))$, then $p \mid k - 1$. Finally, one can show that the only odd primes dividing the resultant $\mathrm{Res}(g_k(X), h_k(X))$ are primes which divide A_k. Indeed, if p is such a prime, then there exist i, j, ℓ such that $\alpha_i^2 \equiv \alpha_j \alpha_\ell \pmod{p}$. The argument from the proof of part (iii) of Theorem 1.1 applies. Namely, we square the relation $\alpha_i - 2 \equiv -\alpha_i^{-k} \pmod{p}$ and multiply the relations $\alpha_s - 1 \equiv \alpha_s^{-k} \pmod{p}$ for $s = j, \ell$ and subtract the two relations, we get that $2\alpha_i \equiv \alpha_j + \alpha_\ell \pmod{p}$. Hence, the quadratic $x^2 - Sx + P \pmod{p}$ has a double root in α_i as well as the roots α_j, α_ℓ modulo p, where $S \equiv 2\alpha_i \pmod{p}$ and $P \equiv \alpha_i^2 \pmod{p}$. Thus, $\alpha_i \equiv \alpha_j \equiv \alpha_s \pmod{p}$. This shows that $p \mid A_k$ (so, $f_k(X)$ has a double root modulo p). Further, because $f_k(X)$ has no triple roots modulo p, we get that we must have $i = j$ to begin with (or $i = \ell$) and then $\alpha_j \equiv \alpha_\ell \pmod{p}$.

Now we consider periods. We use the theory from Chapter 3 in [1]. If $p \nmid A_k(k-1)$, then all the roots of $F_k(X)$ are simple. The number $K(k,p)$ equals the minimal R such that $\alpha_i^R \equiv 1 \pmod{p}$. But, this entails that also $(\alpha_i)^{2R} \equiv (\alpha_i \alpha_j)^R \equiv 1 \pmod{p}$, so $\gamma^R \equiv 1 \pmod{p}$ for all roots γ of $F_k(X)$ modulo p. Hence, $\{g_n^{(k)}\}_{n \ge 0}$ is periodic modulo p with period R.

Assume next that $p \mid A_k$. The polynomial $f_k(X) \pmod{p}$ has only one double root and all other roots are simple. Say α_1 is the double root. Then,

$$F_n^{(k)} = (c_1 + c_2 n)\alpha_1^n + \sum_{i \ge 3}^{k} c_i \alpha_i^n \pmod{p}.$$

Here and elsewhere in this proof, the coefficients c_i and roots α_i are in some appropriate finite extension of $\mathbb{F}_p$. Letting R be minimal such that $\alpha_i^R \equiv 1 \pmod{p}$, we have that $K(k,p) = pR$. Now, let us look at $\{g_n^{(k)}\}_{n \ge 0}$. The polynomial

$$F_k(X) = f_k(X) g_k(X) h_k(X)$$

has one triple root modulo p, several double roots, and several simple roots. Indeed, p does not divide $k - 1$, so $f_k(X)$ and $g_k(X)$ have no roots in common. Also, $f_k(X)$ and $h_k(X)$ have no roots in common modulo p. Thus, there is only one root of $f_k(X)$ that is double modulo p. Say it is α_1. Now for the roots of $g_i(X)h_i(X)$, the root α_1^2 appears at multiplicity 3 (namely as α_1^2, α_2^2 and $\alpha_1\alpha_2$). There are several other roots that appear with multiplicity exactly 2

namely $\alpha_1\alpha_i$ for $i \notin \{3, \ldots, k\}$, and the rest of the roots appear with multiplicity 1. Hence, by the general theory,

$$g_n^{(k)} \equiv \sum_{\substack{\gamma \\ F_k(\gamma) \equiv 0 \pmod{p}}} \sum_{j=1}^{\sigma_\gamma} A_{\gamma,j} \binom{n+j-1}{j-1} \gamma^n \pmod{p},$$

for some coefficients $A_{\gamma,j}$, where σ_j is the multiplicity of γ as a root of $F_k(X)$. Because $\sigma_\gamma \leq 3$, the above binomial coefficients are well defined modulo p and we see that $pK(k,p)$ is also a period of $\{g_n^{(k)}\}_{n\geq 0}$.

Finally, it remains to treat the case $p \mid k-1$. In this case, there is exactly one root of $f_k(X)$ which is 1. Say $\alpha_1 \equiv 1 \pmod{p}$. Then, the only repeated roots of $F_k(X)$ are α_i for $i \in \{2, \ldots, k\}$ (which appear as roots of $f_k(X)$ and as roots of $h_k(X)$) of multiplicity 2, as well as the root $1 = \alpha_1 = \alpha_1^2$, which appears as a root of $f_k(X)$ and $g_k(X)$. So, it also has multiplicity 2 as a root of $F_k(X)$. All other roots of $F_k(X)$ are simple modulo p. It then follows that the period of $\{g_n^{(k)}\}_{n\geq 0}$ is $pK(k,p)$. □

Remark. One can argue that although we proved that the period of $\{g_n^{(k)}\}_{n\geq 0}$ is $pK(k,p)$ for odd primes p dividing $k-1$, it could be that period is shorter and possibly $K(k,p)$. First, we checked it numerically for $k = 6$. We took $p = 5$. Then $K(6,5) = 208$, but calculations showed that the period of $\{g_n^{(k)}\}_{n\geq 1}$ is $1040 = 5 \times 208$. Then, we can argue that the factor p in $pK(k,p)$ is unavoidable. It would be avoidable if in the Binet formula

$$g_n^{(k)} = \sum_{i=1}^{k} c_i \alpha_i^n + \sum_{i=1}^{k} d_i \alpha_i^{2n} + \sum_{1\leq i<j\leq k} e_{i,j} (\alpha_i \alpha_j)^n$$

for $\{g_n^{(k)}\}_{n\geq 0}$, the algebraic numbers c_i, d_i, and $e_{i,j}$ for $1 \leq i \leq k$ and $1 \leq i < j \leq k$ would have denominators coprime to the odd primes $p \mid k-1$. But, this is not so. Let us compute $e_{i,j}$. In

$$g_n^{(k)} - g_{n-1}^{(k)} - \cdots - g_{n-k}^{(k)},$$

the coefficient of $(\alpha_i\alpha_j)^n$ is

$$e_{i,j} \left(1 - \frac{1}{\alpha_i\alpha_j} - \cdots - \frac{1}{(\alpha_i\alpha_j)^k}\right) = e_{i,j} \frac{f_k(\alpha_i\alpha_j)}{(\alpha_i\alpha_j)^k}.$$

On the other hand, in

$$\sum_{j=0}^{k-1} \left(\sum_{i=0}^{j} F_{n-3+i}^{(k)}\right) \left(F_{n-1+j}^{(k)} - F_{n-2+j}^{(k)}\right),$$

this coefficient is

$$S(\alpha_i, \alpha_j) + S(\alpha_j, \alpha_i),$$

where

$$\begin{aligned} S(\alpha_i, \alpha_j) &= \frac{(\alpha_j - 1)}{(\alpha_i\alpha_j)^3} \left(\alpha_j + (1+\alpha_i)\alpha_j^2 + \cdots + (1 + \alpha_i + \cdots + \alpha_i^{k-2})\alpha_j^{k-1}\right) \\ &= \frac{(\alpha_j - 1)}{(\alpha_i\alpha_j)^3} \left(\frac{(\alpha_i\alpha_j) - \alpha_j}{\alpha_i - 1} + \frac{(\alpha_i\alpha_j)^2 - \alpha_j^2}{\alpha_i - 1} + \cdots + \frac{(\alpha_i\alpha_j)^{k-1} - \alpha_j^{k-1}}{\alpha_i - 1}\right) \\ &= \frac{(\alpha_j - 1)}{(\alpha_i\alpha_j)^3(\alpha_i - 1)} \left(-f_k(\alpha_i\alpha_j) + (\alpha_i\alpha_j)^k - \alpha_j^k\right) \end{aligned}$$

$$= \frac{(\alpha_j - 1)}{(\alpha_i\alpha_j)^3(\alpha_i - 1)} \left(-f_k(\alpha_i\alpha_j) + (\alpha_i\alpha_j)^k(\alpha_i - 1)\right)$$
$$= \frac{(\alpha_j - 1)}{(\alpha_i\alpha_j)^k(\alpha_i - 1)} \left(-f_k(\alpha_i, \alpha_j) + f_k(\alpha_i\alpha_j)\left(\frac{\alpha_i\alpha_j - 1}{2(\alpha_j - 1)}\right)\right)$$
$$= \frac{f_k(\alpha_i\alpha_j)(\alpha_j - 1)}{(\alpha_i\alpha_j)^3(\alpha_i - 1)} \left(-1 + \frac{\alpha_i\alpha_j - 1}{2(\alpha_j - 1)}\right).$$

Thus,

$$e_{i,j} = (\alpha_i\alpha_j)^{k-3} \left(-\frac{(\alpha_j - 1)}{\alpha_i - 1} + \frac{\alpha_i\alpha_j - 1}{2}\left(\frac{1}{\alpha_i - 1} + \frac{1}{\alpha_j - 1}\right) - \frac{(\alpha_i - 1)}{\alpha_j - 1}\right).$$

The factor in parenthesis can be simplified as

$$\frac{-2(\alpha_i - 1)^2 - 2(\alpha_j - 1)^2 + (\alpha_i\alpha_j - 1)(\alpha_i + \alpha_j - 2)}{(\alpha_i - 1)(\alpha_j - 1)}.$$

If p is odd and divides $k - 1$, then the ideals $\pi_i := \gcd(\alpha_i - 1, p)$ and $\pi_j := \gcd(\alpha_j - 1, p)$ of $\mathcal{O}_{\mathbb{K}}$ are coprime. If not, their greatest common divisor will divide p, so $k - 1$, and $\alpha_i - \alpha_j$, so A_k, which is impossible by Lemma 2.1. Further, they are conjugated and their product is a multiple of p, so none is a unit. Because the numerator of the above expression is congruent to $-(\alpha_j - 1)^2 \pmod{\alpha_i - 1}$ and also to $-(\alpha_i - 1)^2 \pmod{\alpha_j - 1}$, it follows that π_i and π_j are coprime to the numerator of the above expression. Hence, p appears in the prime ideal factorization of the denominator of $e_{i,j}$ at a negative power. This explains why the factor of p in the period $pK(K, p)$ for p odd dividing $k - 1$ cannot be avoided.

Acknowledgment

The author thanks the referee for a careful reading of the paper and useful comments.

References

[1] G. Everest, A. van der Poorten, I. E. Shparlinski, and T. Ward, *Recurrence Sequences*, Mathematical Surveys and Monographs, **104**, American Mathematical Society, Providence, RI, 2003.

[2] C. A. Gómez, J. C. Gómez, and F. Luca, *Multiplicative dependence between k-Fibonacci and k-Lucas numbers*, Periodica Math. Hungarica (to appear).

[3] M. Hashemi and M. Pirzadeh, *The t-Fibonacci sequences in some finite groups with centre $Z(G) = G'$*, J. Combinatorial Mathematics and Combinatorial Computing (to appear).

[4] P. A. Martin, *The Galois group of $x^n - x^{n-1} - \cdots - 1$*, J. Pure App. Algebra, **190** (2004), 213–223.

[5] M. Mignotte, *Sur les conjugués des nombres de Pisot*, C. R. Acad. Sci. Paris Sér. I Math., **298** (1984), 21.

[6] R. M. Murty and J. Esmonde, *Problems in Algebraic Number Theory*, 2nd ed., Graduate Texts in Mathematics, **190**, Springer-Verlag, New York, 2005.

MSC2020: 11B39.

School of Mathematics, University of the Witwatersrand, Private Bag X3, WITS 2050, Johannesburg, South Africa, Research Group in Algebraic Structures and Applications, King Abdulaziz University, Jeddah, Saudi Arabia, Centro de Ciencias Matemáticas, UNAM, Morelia, Mexico

Email address: florian.luca@wits.ac.za