An. Şt. Univ. Ovidius Constanţa Vol. 9(1), 2001, 27–38

ON THE GALOIS GROUP OF THE GENERALIZED FIBONACCI POLYNOMIAL

Mihai Cipu* and Florian Luca

1 Statements of Results

For every integer $n \geq 2$ let

$$f_n(X) = X^n - X^{n-1} - \ldots - X - 1 \in \mathbb{Z}[X] \tag{1}$$

be the *generalized Fibonacci polynomial.* There are a few papers in the literature in which the distribution of the roots of f_n is considered. For example, from [5] and [6] we know that there exists a unique positive root θ of f_n, which is larger than 1, and all the other roots of f_n have modulus less than 1. Moreover, if n is odd, then f_n has only one real root, while if n is even, f_n has exactly two real roots (the root $\theta > 1$ and one other root in the interval $(-1, 0)$). For an analysis of the real roots of f_n' and f_n'' see [3].

Since f_n has a unique positive root θ which is larger than 1 and all the other roots are in the open unit disk, it follows that θ is a *Pisot number* and f_n is a Pisot polynomial. In particular, f_n is irreducible. This observation is due to Boyd (see [9]). Thus, we may denote the roots of f_n by $\theta^{(i)}$ for $i = 1, 2, \ldots, n$, with the usual convention that $\theta^{(1)} = \theta$. We also let $n = r_1 + 2r_2$, where r_1 is the number of real roots of f_n and $2r_2$ is the number of complex non-real roots of f_n. From the above comments we know that $r_2 = \left\lfloor \frac{n-1}{2} \right\rfloor$. We also number the roots $\theta^{(i)}$ with the usual convention, namely that $\theta^{(r_1+j)} = \overline{\theta}^{(r_1+r_2+j)}$ for all $j = 1, 2, \ldots, r_2$. From the general theory of Pisot numbers, we can immediately infer a few facts about the numbers $\theta^{(i)}$ which, to our knowledge, were not yet pointed out in the context of the polynomial f_n. First of all, from a result of Smyth (see [7]), it follows that $|\theta^{(i)}| \neq |\theta^{(j)}|$ if $1 \leq i < j \leq r_1 + r_2$. In particular, the only coincidences among the absolute values of the $\theta^{(i)}$'s

Received: November, 2001.

*Partially supported by ANSTI Grant 5232 are the trivial ones. Moreover, by a result of Mignotte (see [4]), it follows that the set $\{\theta^{(i)} : i = 2, 3, \ldots, n\}$ consists of multiplicatively independent numbers. Notice also that since the constant term of f_n is -1, it follows that the numbers $\theta^{(i)}$ are all units. Recall that an algebraic number α is called unit if both α and $1/\alpha$ are algebraic integers.

In [9] it was raised the question to compute the Galois group G_n of the polynomial f_n over the field of rational numbers. This group was computed using MAGMA (see [9]) for all $n \leq 11$ and it was found to be the symmetric group S_n. This led the author of [9] to conjecture that the Galois group $G_n = \mathrm{Gal}(f_n, \mathbb{Q})$ is S_n for all n. The question of computing G_n was raised in the context of finding the roots of f_n by using radicals, which is equivalent to the solvability of the group G_n.

In this paper we make some remarks on the Galois group G_n. We show that G_n is not contained in the alternating group A_n for any n, and is not 2-nilpotent for $n \geq 3$.

Our main result leaves open both possibilities to settle the conjecture. To the best of our knowledge, it is the only general result valid for all polynomials f_n's.

Theorem 1.1 *The Galois group G_n is not contained in the alternating group A_n (here we view G_n as contained in S_n).*

The proof we shall give to this result works equally well for other polynomials. Thus we have:

Theorem 1.2 *The Galois group* $\mathrm{Gal}(u_n, \mathbb{Q})$ *of the polynomial*

$$u_n(X) := X^n + X^{n-1} - X^{n-2} - \ldots - X - 1 \ , \ n \geq 4,$$

is contained in the alternating group A_n if and only if $n \equiv 3 \pmod 4$.

For the generalized Fibonacci polynomial we prove also:

Theorem 1.3 *For $n \geq 3$, the Galois group G_n is not 2-nilpotent.*

From this result it follows that the roots of the generalized Fibonacci polynomials f_n, $n \geq 3$, can not be constructed by ruler and compass.

It is well-known folklore that in general the arithmetic over the ring of integers $\mathbb{Z}$ is a lot harder than the arithmetic over the function field $\mathbb{Q}(t)$. In particular, statements such as Fermat's Last Theorem, or binary Goldbach's Conjecture, or ABC Conjecture, which are notoriously hard over the integers, admit very easy proofs over the function field. In this paper we give another example of this phenomenon.

Theorem 1.4 *Let t be algebraically independent over $\mathbb{Q}(X)$. The Galois group of the polynomial $g := -X^n f_n(1/X) - t$ over $\mathbb{Q}(t)$ is S_n.*

2 Proofs

Recall that if $f \in \mathbb{Z}[X]$ is any polynomial of degree $d \geq 2$ and of roots $\alpha_1, \alpha_2, \ldots, \alpha_d$ (not necessarily distinct), then the *discriminant of f* is defined as

$$D(f) := \prod_{1 \leq i < j \leq d} (\alpha_i - \alpha_j)^2 \ . \tag{2}$$

This definition requires the knowledge of all the roots of the given polynomial, which is in general a difficult task. The discriminat can be computed as the resultant of the polynomial and of its derivative.

For the proof of Theorem 1.1 we use the well-known criterion: the Galois group of a polynomial of degree n is contained in the alternating group A_n if and only if the discriminant of the polynomial is a perfect square in the base field. So we need the value of the discriminant of the generalized Fibonacci polynomial.

Lemma 2.1 *Let D_n be the discriminant of f_n. Then*

$$D_n = (-1)^{(n-1)(n-2)/2} \cdot \frac{2^{n+1}n^n - (n+1)^{n+1}}{(n-1)^2} \ . \tag{3}$$

Remark 2.1 *Notice that if one substitutes $n = 2$ in the above expression, then one obtains the familiar $D_2 = 5$.*

In all the proofs we will not actually work with polynomial f_n but rather with its reciprocal polynomial, namely

$$g_n(X) := -X^n f\left(\frac{1}{X}\right) = X^n + X^{n-1} + \ldots + X - 1 \ . \tag{4}$$

It is clear that by replacing f_n by g_n we do not change the Galois group G_n. Moreover, since the product of the roots of f_n is ±1, and since the roots of g_n are the reciprocals of the roots of f_n, formula (2) shows that the discriminant of g_n is D_n as well.

We are now ready to prove Lemma 2.1.

Proof of Lemma 2.1.

For the sake of convenience, we drop the index n appearing at the polynomial g_n. We also denote by $\beta_i = 1/\theta^{(i)}$ for $i = 1, 2, \ldots, n$ the roots of the polynomial g. Notice that

$$g(X) = \sum_{i=0}^{n} X^i - 2 = \frac{X^{n+1} - 1}{X - 1} - 2 = \frac{X^{n+1} - 2X + 1}{X - 1} \ . \tag{5}$$

Let us consider the polynomial appearing as the numerator of the last expression:

$$h(X) := X^{n+1} - 2X + 1 \ . \tag{6}$$

Formula (5) can be rewritten as

$$(X-1)g(X) = h(X) \ . \tag{7}$$

Taking derivatives in both sides of equation (7) and then evaluating the resulting expression in β_i for $i = 1, 2, \ldots, n$, we get

$$(\beta_i - 1)g'(\beta_i) = h'(\beta_i) \ , \quad \text{for } i = 1, 2, \ldots, n. \tag{8}$$

Taking the product of all expressions (8) for $i = 1, 2, \ldots, n$, and rearranging some factors we get

$$\prod_{i=1}^{n} g'(\beta_i) = (-1)^n \cdot \frac{\prod_{i=1}^{n} h'(\beta_i)}{\prod_{i=1}^{n}(1-\beta_i)}. \tag{9}$$

It is easily seen that the denominator appearing in the right-hand side of formula (9) is $g(1) = n - 1$. Moreover, from formula (7) we see that the roots of h are precisely the numbers β_i for $i = 1, 2, \ldots, n$ together with $\beta_{n+1} := 1$. Since $h'(1) = n - 1$, it follows that one may rewrite formula (9) as

$$\prod_{\beta \,|\, g(\beta)=0} g'(\beta) = \frac{(-1)^n}{(n-1)^2} \prod_{\gamma \,|\, h(\gamma)=0} h'(\gamma). \tag{10}$$

It is well-known that if f is any polynomial with rational coefficients, then its discriminant can be computed using the formula

$$D(f) = (-1)^{r_2} \prod_{\alpha \,|\, f(\alpha)=0} |f'(\alpha)|. \tag{11}$$

From formulae (10) and (11) it follows that

$$|D_n| = \prod_{\beta \,|\, g(\beta)=0} |g'(\beta)| = \frac{1}{(n-1)^2} \prod_{\gamma \,|\, h(\gamma)=0} |h'(\gamma)| = \frac{|D_n|}{(n-1)^2}. \tag{12}$$

Hence, it suffices to compute the discriminant of the polynomial h. However, it is well-known that if $f \in \mathbb{Z}[X]$ is a polynomial of the form

$$f(X) = X^n + aX + b \ , \tag{13}$$

then its discriminat satisfies

$$|D(f)| = |n^n b^{n-1} + a^n (1-n)^{n-1}| \tag{14}$$

(see, for instance, Ex. 4.5.4 on page 48 in [2]). Using formulae (6) and (14), we get

$$\begin{array}{rcl} |D(h)| & = & |(n+1)^{n+1} + (-2)^{n+1}(1-(n+1))^n| \\ & = & |(n+1)^{n+1} + (-1)^{2n+1} \cdot 2^{n+1} n^n| \\ & = & 2^{n+1} n^n - (n+1)^{n+1}. \end{array} \tag{15}$$

Hence,

$$|D_n| = \frac{2^{n+1} n^n - (n+1)^{n+1}}{(n-1)^2}. \tag{16}$$

It remains to establish the sign of D_n. But this is $(-1)^{r_2}$, where $r_2 = \left\lfloor \frac{n-1}{2} \right\rfloor$, and it is easy to see that

$$\left\lfloor \frac{n-1}{2} \right\rfloor \equiv \binom{n-1}{2} = \frac{(n-1)(n-2)}{2} \pmod 2 \ , \quad \text{for all } n \in \mathbb{Z}. \tag{17}$$

Formula (3) is therefore proved. ∎

Proof of Theorem 1.1.

According to the criterion recalled before the proof of Lemma 2.1, in order to establish Theorem 1.1, it suffices to show that D_n is never a square, where D_n is given by formula (3). Since $D_n < 0$ when $n \equiv 0\,,\,3 \pmod 4$, it is sufficient to treat the cases $n \equiv 1\,,\,2 \pmod 4$.

Case 1. $n \equiv 1 \pmod 4$

The fact that D_n is a square is equivalent to

$$2^{n+1}\left(n^n - \left(\frac{n+1}{2}\right)^{n+1}\right) = x^2 \tag{18}$$

for some positive integer x. From equation (18) we conclude that one may write $x = 2^{(n+1)/2} y$ for some positive integer y which satisfies

$$n^n - \left(\frac{n+1}{2}\right)^{n+1} = y^2. \tag{19}$$

Since $n \equiv 1 \pmod 4$, equation (19) reduced modulo 4 shows that y is even. We now rewrite (19) as

$$\begin{array}{rcl} n^n & = & y^2 + \left(\frac{n+1}{2}\right)^{n+1} \\ & = & \left(y + i\left(\frac{n+1}{2}\right)^{(n+1)/2}\right) \cdot \left(y - i\left(\frac{n+1}{2}\right)^{(n+1)/2}\right). \end{array} \tag{20}$$

Since n is odd, y is even and n and $n+1$ are coprime, it follows that the two conjugate factors appearing in the right-hand side of equation (20) are coprime in the ring of Gaussian integers $\mathbb{Z}[i]$. Since $\mathbb{Z}[i]$ is an Euclidian ring, it follows that there exist an integer $\omega \in \mathbb{Z}[i]$ and a unit $\zeta \in \mathbb{Z}[i]$ such that $\omega \cdot \overline{\omega} = n$ and

$$\left\{ \begin{array}{rcl} \zeta\omega^n & = & y + i\left(\dfrac{n+1}{2}\right)^{(n+1)/2} , \\ \overline{\zeta}\overline{\omega}^n & = & y - i\left(\dfrac{n+1}{2}\right)^{(n+1)/2} . \end{array} \right. \tag{21}$$

Since the only units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$ of order dividing 4 and n is odd, it follows that, via an appropriate substitution, we may assume that $\zeta = 1$. With this assumption, we eliminate y from the equation (21) obtaining

$$\frac{\omega^n - \overline{\omega}^n}{\omega - \overline{\omega}} = \frac{i(n+1)^{(n+1)/2}}{2^{(n-1)/2}(\omega - \overline{\omega})} . \tag{22}$$

Notice that the left-hand side of equation (22) is the nth term of a Lucas sequence of first kind with roots ω and $\overline{\omega}$. The right-hand side of equation (22) is therefore a rational integer as well, and its prime factors divide $n+1$. In particular, the largest prime dividing the number appearing in either side of formula (22) is at most

$$P(n+1) \leq \frac{n+1}{2} < n-1 , \quad \text{for } n \geq 5 . \tag{23}$$

Here, for a positive integer $K > 1$ we have denoted by $P(k)$ the largest prime divisor of k. In particular, inequality (23) implies that the Lucas number appearing in the left-hand side of equation (22) has no primitive divisors. The Lucas numbers without primitive divisors have been completely classified recently by Bilu, Hanrot and Voutier (see [1]). There are none with $n > 13$ odd, there are only a few with $5 \leq n \leq 13$ odd, and all of these appear in Table 1 in [1]. A quick look at the Table 1 in [1] suffices to notice that none of these defective Lucas numbers has roots belonging to the ring of Gaussian integers. Hence, the Diophantine equation (22) has no solutions.

Case 2. $n \equiv 2 \pmod 4$.

We can treat this case in an elementary way. Assume that x is a positive integer such that

$$2^{n+1}n^n - (n+1)^{n+1} = x^2 . \tag{24}$$

Let p be any prime divisor of $n+1$. Reducing equation (24) modulo p and using the fact that n is even, we get $\left(\frac{2}{p}\right) = 1$. (For any integers a and b with

b odd we denote by $\left(\frac{a}{b}\right)$ the Jacobi symbol of a with respect to b.) Hence, $p \equiv \pm 1 \pmod 8$. Since this holds for all prime divisors of the odd number $n+1$, we conclude that $n+1 \equiv \pm 1 \pmod 8$. However, since $n+1 \equiv 3 \pmod 4$, it follows that $n+1 \equiv 7 \pmod 8$.

Notice now that $n/2$ is an odd number. Let q be any prime divisor of it. Reducing equation (24) modulo q, we get

$$\left(\frac{-(n+1)}{q}\right) = 1 \ .$$

Since q is a divisor of n, we conclude $\left(\frac{-1}{q}\right) = 1$, which implies that $q \equiv 1 \pmod 4$. Since this holds for all odd prime divisors of n, it results $n/2 \equiv 1 \pmod 4$, or $n \equiv 2 \pmod 8$. This leads to $n+1 \equiv 3 \pmod 8$, which contradicts the previous conclusion that $n+1 \equiv 7 \pmod 8$. This concludes the proof of Theorem 1.1. ■

Proof of Theorem 1.2.

The pattern of the proof is as above. We start by computing the discriminant of the polynomials we are interested in.

Lemma 2.2 *For $n \geq 4$, the discriminant of u_n has absolute value*

$$\mid \mathrm{Disc}(u_n) \mid = \begin{cases} \dfrac{2^{n+3}(n-1)^{n-1} - (n+1)^{n+1}}{(n-3)^2} & \text{for } n \text{ even,} \\[2ex] \left(\dfrac{(n+1)^{(n+1)/2} - 2^{(n+3)/2}(n-1)^{(n-1)/2}}{n-3}\right)^2 & \text{for } n \text{ odd,} \end{cases}$$

and sign $(-1)^{(n+1)(n+2)/2}$.

We proceed to the proof of Theorem 1.2. Since the discriminant of u_n is negative for $n \equiv 0\,,\ 1 \pmod 4$, for these values of n certainly $\mathrm{Disc}(u_n)$ is not the square of an integer. For $n \equiv 3 \pmod 4$ $\mathrm{Disc}(u_n)$ is a perfect square, so it remains to consider tha case $n \equiv 2 \pmod 4$.

Assume that x is an integer such that

$$2^{n+3}(n-1)^{n-1} - (n+1)^{n+1} = x^2 \ . \tag{25}$$

Reducing equation (25) modulo 8 we get $n \equiv 6 \pmod 8$. Hence, $n+1$ has a prime divisor p congruent to 3 modulo 4. Reducing equation (25) modulo p and using the fact that n is even we get

$$\left(\frac{-1}{p}\right) = 1 \ ,$$

which contradicts the previous conclusion that $p \equiv 3 \pmod 4$. Therefore, the Diophantine equation (25) has no solutions for $n \equiv 2 \pmod 4$.

This concludes the proof of Theorem 1.2. ∎

Proof of Lemma 2.2.

The familiar Sylvester determinant does not provide the simplest way to compute the discriminant of u_n as the resultant of u_n and of its derivative. We shall use the fortunate fact that the reciprocal of u_n has a sparse multiple

$$v_{n+1}(X) := X^n(1-X)u_n\left(\frac{1}{X}\right) = X^{n+1} - 2X^{n-1} + 1 \ .$$

Then

$$\begin{aligned}\mathrm{Disc}(v_{n+1}) &= \mathrm{Disc}((X-1)u_n) = \mathrm{Disc}(u_n)\cdot \mathrm{Res}(X-1, u_n(X))^2 \\ &= (n-3)^2\,\mathrm{Disc}(u_n) \ .\end{aligned}$$

For the sake of simplicity, in the following we shall fix a value n and we put $v := v_n$. We have

$$\begin{aligned}\mid \mathrm{Disc}(v) \mid &= \mid \mathrm{Res}(v, v') \mid = \prod_{v(\rho)=0} \mid n\rho^{n-1} - 2(n-2)\rho^{n-3} \mid \\ &= \prod_{v(\rho)=0} \mid n\rho^2 - 2n + 4 \mid \\ &= \pm n^n v\left(\sqrt{2-4/n}\right) v\left(-\sqrt{2-4/n}\right) \ .\end{aligned}$$

For n even one has

$$v\left(\sqrt{2-4/n}\right) = v\left(-\sqrt{2-4/n}\right) = 1 - \frac{4}{n}\left(2-\frac{4}{n}\right)^{n/2-1} \ ,$$

so that

$$\mid \mathrm{Disc}(v) \mid = \left(n^{n/2} - 2^{n/2+1}(n-2)^{n/2-1}\right)^2 \ .$$

For n odd

$$\begin{aligned}v\left(\sqrt{2-4/n}\right) &= 1 - \frac{4}{n}\left(2-\frac{4}{n}\right)^{n/2-1} \ , \\ v\left(-\sqrt{2-4/n}\right) &= 1 + \frac{4}{n}\left(2-\frac{4}{n}\right)^{n/2-1} \ .\end{aligned}$$

Hence,

$$\mid \mathrm{Disc}(v) \mid = 2^{n+2}(n-2)^{n-2} - n^n \ .$$

Notice that the right-hand side of the previous relation is non-negative for every $n \geq 4$.

From these computations it follows that the discriminat of u_n has absolute value

$$| \operatorname{Disc}(u_n) |= \begin{cases} \dfrac{2^{n+3}(n-1)^{n-1}-(n+1)^{n+1}}{(n-3)^2} & \text{for } n \text{ even },\\ \dfrac{\left(2^{(n+3)/2}(n-1)^{(n-1)/2}-(n+1)^{(n+1)/2}\right)^2}{(n-3)^2} & \text{for } n \text{ odd }. \end{cases}$$

By Descarte's rule of sign, v_{2n} has 0 or 2 positive real roots and 0 or 2 negative real roots. Since $v_{2n}(\pm 1) = 0$, we conclude that v_{2n} has exactly 4 real roots. Similarly on finds that v_{2n+1} has precisely 3 real roots. Hence, the sign of $\operatorname{Disc}(u_n)$ is $(-1)^{r_2}$, where $r_2 = \lfloor n/2 \rfloor - 1$. It is easily seeen that this coincides with $(-1)^{(n+1)(n+2)/2}$.

Lemma 2.2 is therefore proved. ∎

Proof of Theorem 1.3.

Assume that the group G_n is 2-nilpotent and write $G_n = S \times T$, where S is the 2-Sylow subgroup of G_n and T is a subgroup of odd order. For any root θ of f_n write $\mathbf{K}_\theta := \mathbb{Q}[\theta]$ and let $\mathbf{K}$ be the splitting field of f_n. Notice that since $n \geq 3$, the polynomial f_n has complex non-real roots therefore S is non-trivial (the complex conjugation is an example of an element of order two in G_n). Let θ be any root of f_n. It is clear that $\operatorname{Stab}_{G_n}(\theta)$ does not contain S. Indeed, for if $S \leq \operatorname{Stab}_{G_n}(\theta)$, then, by the normality of S, it would follow that $S \subseteq \cap_{f_n(\theta)=0} \operatorname{Stab}_{G_n}(\theta) = \{1\}$, which is impossible because S is non-trivial. Let N be a maximal subgroup of S containing $S \cap \operatorname{Stab}_{G_n}(\theta)$ and let $M = N \times T$. Since N is maximal in the 2-group S, we get that N is normal in S and $[S : N] = 2$. Clearly, M is a normal subgroup of index 2 in G_n and contains $\operatorname{Stab}_{G_n}(\theta)$ for every root θ of f_n. By Galois correspondence, $\mathbf{K}_1 := \mathbf{K}^M$ is a number field of degree 2 which is contained in each one of the fields $\mathbf{K}_\theta$. In particular, $n = 2m$ is even and f_n decomposes over $\mathbf{K}_1$ into two polynomials, say g_n and h_n, each of degree m. We keep θ_1 as the only root of f_n which is outside the unit disc and we reorder the roots $\theta_2, \ldots, \theta_n$ such that $\theta_1, \ldots, \theta_m$ are the roots of g_n and $\theta_{m+1}, \ldots, \theta_{2m}$ are the roots of h_n. We also write $\mathbf{K}_1 = \mathbb{Q}[\sqrt{d}]$ for some squarefree integer $d \neq 1$. Let c_g and c_h be the last two coefficients of g_n and h_n, respectively. Since $c_g = (-1)^m \theta_1 \cdot \cdots \cdot \theta_m$ and $c_h = (-1)^m \theta_{m+1} \cdot \cdots \cdot \theta_n$ and $c_g \cdot c_h = -1$, it follows that c_g and c_h are both units in $\mathbf{K}_1$ and $c_g = -c_h^{-1}$. Assume first that $d < 0$. Then all the units in $\mathbf{K}_1$ are roots of unity of degrees 1, 2, 3, or 6, therefore we read that $c_g^{12} = 1$. In particular, $(\theta_1 \cdot \cdots \cdot \theta_m)^{12} = 1$, which is impossible either by the result of Mignotte, or simply by noticing that since $\theta_1 \cdot \cdots \cdot \theta_n = 1$, it follows that $|c_g| = |\theta_1 \cdot \cdots \cdot \theta_m| = |\theta_{m+1} \cdot \cdots \cdot \theta_n|^{-1} > 1$. So, we conclude that $d > 0$, therefore $\mathbf{K}_1$ is real. Let ζ be a fundamental unit in $\mathbf{K}_1$. Since $|c_g| > 1$, we get that $c_g = \pm\zeta^t$ for some positive integer t. However, it is easy to see that $\theta_1 < 2$, therefore $|c_g| < 2$. We now get that $|\zeta|^t = |c_g| < 2$, and the only instance that this can happen in a quadratic number field is when $t = 1$ and $d = 5$, for which $\zeta = (1+\sqrt{5})/2$. Since we now know that $d = 5$, we get that the discriminant of $\mathbf{K}_1$ is $D_{\mathbf{K}_1} = 5$, and since $\mathbf{K}_1 \subset \mathbf{K}_\theta$ and $[\mathbf{K}_\theta : \mathbf{K}_1] = m$ we read that $D_{\mathbf{K}_1}^m \mid D_n$, therefore $5^{n/2} \mid D_n$. Notice that by the Claim below this is impossible when $n \equiv 1 \pmod 5$.

Claim. *If p is an odd prime dividing $n-1$, then p does not divide D_n.*

To prove this Claim, we compute the numerator of D_n modulo $(n-1)^3$:

$$2^{n+1}n^n - (n+1)^{n+1} = 2^{n+1}((n-1)+1)^n - ((n-1)+2)^{n+1}$$

$$\equiv 2^{n+1}\left(\binom{n}{2}(n-1)^2 + n(n-1) + 1\right)$$

$$-\left(\binom{n+1}{2}2^{n-1}(n-1)^2 + (n+1)(n-1)2^n + 2^{n+1}\right) \pmod{(n-1)^3}$$

$$\equiv 2^{n-1}(n-1)^2 \pmod{(n-1)^3}\ .$$

The above computation together with formula (3) show that

$$D_n \equiv (-1)^{\binom{n-1}{2}}2^{n-1} \pmod{(n-1)}\ ,$$

whence our Claim.

We resume the proof of Theorem 1.3. We now distinguish two cases:

Case 1. $n \equiv 0 \pmod 4$.

Since $5^{n/2} \mid D_n$, we get $2^{n+1}n^n - (n+1)^{n+1} \equiv 0 \pmod 5$. It is clear that $n \not\equiv 0,\ 4 \pmod 5$ and since $n \equiv 0 \pmod 4$ it follows, by Fermat's Little Theorem, that $2^{n+1}n^n - (n+1)^{n+1} \equiv 2 - (n+1) \pmod 5$ leading to $n \equiv 1 \pmod 5$, which we have seen that it is impossible.

Case 2. $n \equiv 2 \pmod 4$.

In this case, we get again that $n \equiv 0,\ 4 \pmod 5$ are not possible, and with Fermat's Little Theorem we obtain $2^{n+1}n^n - (n+1)^{n+1} \equiv 8n^2 - (n+1)^3 \pmod 5$ and the only solution $n \not\equiv 1 \pmod 5$ of $8n^2 - (n+1)^3 \equiv 0 \pmod 5$ is $n \equiv 2 \pmod 5$. So, we get that $n \equiv 2 \pmod{20}$, and now since $20 = \phi(25)$ we get, with $n = 2 + 20k$,

$$2^{n+1}n^n - (n+1)^{n+1} \equiv 2^3 \cdot (2+20k)^2 - (3+20k)^3 \pmod{25},$$

therefore

$$2^{n+1}n^n - (n+1)^{n+1} \equiv 8(4+80k) - (27+540k) \pmod{25},$$

or

$$2^{n+1}n^n - (n+1)^{n+1} \equiv 5 + 100k \pmod{25} \equiv 5 \pmod{25},$$

which shows that the divisibility relation $5^{n/2} \mid D_n$ is impossible for $n > 2$.

The Theorem is therefore proved. ■

Proof of Theorem 1.4.

We shall use a criterion going back to Hilbert: the polynomial does not take the same value when evaluated for distinct roots of its derivative (see [8, Theorem 3.6])

Let α and β be distinct roots of g' (here the derivative is taken with respect to X). Taking derivatives in both sides of equation (7) and then evaluating the resulting expression in α and β, we conclude that $g(\alpha) = (n+1)\alpha^n - 2$ and $g(\beta) = (n+1)\beta^n - 2$ coincide if and only if $c := \alpha/\beta$ is an nth root of unity. Since

$$g'(X) = \frac{nX^{n+1} - (n+1)X^n + 1}{(1-X)^2},$$

from $g'(\beta) = g'(c\beta) = 0$ and c an nth root of unity it readily follows $c = 1$, which contradicts $\alpha \neq \beta$. ■

References

[1] Y. Bilu, G. Hanrot, and P. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers*, J. Reine und Angew. Math., **539**(2001), 75-122.

[2] J. Esmonde and M. R. Murty, *Problems in Algebraic Number Theory*, Springer-Verlag, New York, 1999.

[3] G. W. Grossman and S. K. Narayan, *On the characteristic polynomial of the j-th order Fibonacci sequence*, in Applications of Fibonacci Numbers, vol. 8, Kluwer Academic Publishers, 1999, 165–178.

[4] M. Mignotte, *Sur les conjugués des nombres de Pisot*, C. R. Acad. Sci. Paris, Sér. I Math., **298**(1984), no. 2, 21.

[5] E. P. Miles, *Generalized Fibonacci numbers and associated matrices*, Amer. Math. Monthly, **67**(1960), 745–752.

[6] M. D. Miller, *On generalized Fibonacci numbers*, Amer. Math. Monthly, **78**(1971), 1008–1009.

[7] C. J. Smyth, Problem 5931, Amer. Math. Monthly, **82**(1975), 86.

[8] G. Turnwald, *On Schur's conjecture*, J. Austral. Math. Soc. Ser. A, **58**(1995), 312–357.

[9] D. Wolfram, *Solving generalized Fibonacci recurrences*, Fibonacci Quart., **36**(1998), 129–145.

Institute of Mathematics
of the Romanian Academy,
P. O. Box 1-764,
RO-70109 Bucharest,
Romania
e-mail:Mihai.Cipu@imar.ro

Instituto de Matematicas de la UNAM,
Campus Morelia,
Ap. Postal 61-3(Xangari), CP 58 089,
Morelia, Michoacán,
Mexico
E-mail: fluca@matmor.unam.mx