Sitzungsber. Abt. II (2005) 214: 81–88

Sitzungsberichte
Mathematisch-naturwissenschaftliche Klasse Abt. II
Mathematische, Physikalische und Technische Wissenschaften

On the Indecomposability of Polynomials*

By

Andrej Dujella, Ivica Gusić, and **Robert F. Tichy**

(Vorgelegt in der Sitzung der math.-nat. Klasse am 13. Oktober 2005
durch das k. M. Robert F. Tichy)

Abstract

Applying a combinatorial lemma a new sufficient condition for the indecomposability of integer polynomials is established.

Mathematics Subject Classification (2000): 11C08, 11B39, 12E05.
Key words: Polynomials with integer coefficients, indecomposability, Fibonacci polynomials.

1. Introduction

In [3], BILU and TICHY proved an explicit finiteness criterium for the polynomial Diophantine equation $f(x) = g(y)$. Their result generalizes a previous one due to SCHINZEL [8, Theorem 8], who gave a finiteness criterium under the assumption $(\deg f, \deg g) = 1$, see also [9]. These criteria are closely connected with decomposability properties of the polynomials f and g. A polynomial $f \in \mathbb{C}[x]$ is called *indecomposable* (over $\mathbb{C}$) if $f = g \circ h$, $g, h \in \mathbb{C}[x]$ implies $\deg g = 1$ or $\deg h = 1$. Two decompositions of f, say $f = g_1 \circ h_1$ and $f = g_2 \circ h_2$ are *equivalent* if there exists a linear function L such that $g_2 = g_1 \circ L$, $h_2 = L^{-1} \circ h_1$ (see [8, pp. 14–15]).

* Dedicated to W. G. NOWAK on the occasion of his 50th birthday.

The criterium of BILU and TICHY has been already applied to several Diophantine equations of the form $f_n(x) = g_m(y)$, where (f_n) and (g_n) are sequences of classical polynomials (see [1, 2, 5, 7, 10–12]). In these results, the indecomposability of corresponding polynomials was usually proved using some analytical properties of these polynomials. In particular, in [5], the equation $F_m(x) = F_n(y)$ was considered, where (F_n) is the sequence of Fibonacci polynomials defined by $F_0(x) = 0$, $F_1(x) = 1$, $F_{n+1} = xF_n(x) + F_{n-1}$ for $n \geq 1$. It was proved that F_n is indecomposable for even n, while for n odd there is only one (up to equivalence) decomposition of F_n. In [4], general criteria for indecomposability of polynomials were obtained in terms of the degree and two leading coefficients. In particular, the above-mentioned result from [5] now follows from the fact that $F_n(x) = x^{n-1} + (n-2)x^{n-3} + \cdots$ and $\gcd(n-1, n-2) = 1$.

In this paper, we will show that from these assumptions on the degree and on the leading coefficients it is possible to obtain much stronger conclusions related to the indecomposability of the polynomial.

2. Results

Lemma 1. *Let $l \geq 2$. Denote by Y the set of all l-tuples $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_l)$ of nonnegative integers satisfying*

$$\alpha_1 \cdot 1 + \alpha_2 \cdot 2 + \cdots + \alpha_l \cdot l = l, \qquad 1 \leq \alpha_1 + \alpha_2 + \cdots + \alpha_l \leq m. \tag{2.1}$$

Then

$$\sum_{\alpha \in Y} \frac{(m-1)!}{(m - \sum_{i=1}^{l} \alpha_i)!} \cdot \frac{l!}{\prod_{i=1}^{l} \alpha_i! \cdot \prod_{i=1}^{l} (i!)^{\alpha_i}} = m^{l-1}.$$

Proof. Let us denote by $S(l,j)$ the Stirling number of the second kind, i.e. the number of ways to partition a set of l elements into j nonempty subsets. If we denote by α_i the number of subsets with i elements, we immediately obtain the following formula:

$$\sum_{\substack{\alpha \in Y \\ \alpha_1 + \cdots + \alpha_l = j}} \frac{l!}{\prod_{i=1}^{l} \alpha_i! \cdot \prod_{i=1}^{l} (i!)^{\alpha_i}} = S(l,j). \tag{2.2}$$

It is well known (see e.g. [6, Sect. 6.1]) that the Stirling numbers satisfy the recurrence

$$S(l,0) = 0, \qquad S(l,j) = S(l-1,j-1) + jS(l-1,j) \qquad \text{for} \quad j \geq 1,$$

and the summation formula

$$\sum_{j=0}^{l} x(x-1)(x-2)\cdots(x-j+1)S(l,j) = x^l. \tag{2.3}$$

Note that if $x = m$, where m is a nonnegative integer, then the terms with $j > m$ in (2.3) vanish. Also, $S(l,j) = 0$ for $j > l$. Therefore, we have

$$\sum_{j=0}^{m} \frac{m!}{(m-j)!} S(l,j) = m^l. \tag{2.4}$$

Applying formulas (2.2) and (2.4), we obtain

$$\sum_{\alpha \in Y} \frac{(m-1)!}{(m-\sum_{i=1}^{l}\alpha_i)!} \cdot \frac{l!}{\prod_{i=1}^{l}\alpha_i! \cdot \prod_{i=1}^{l}(i!)^{\alpha_i}} = \sum_{j=1}^{m} \frac{(m-1)!}{(m-j)!} S(l,j) = m^{l-1}.$$

■

Theorem 1. *Let* $f(x) = x^n + a_{n-1}x^{n-1} + \cdots + a_0 \in \mathbb{Z}[x]$ *and* $h(x) = x^k + c_{k-1}x^{k-1} + \cdots + c_0 \in \mathbb{C}[x]$, $k \geq 2$. *Assume that*

$$f(x) = (h(x))^m + b \cdot (h(x))^{m-1} + H(x), \tag{2.5}$$

with $b \in \mathbb{C}$, $H(x) \in \mathbb{C}[x]$ *and* $\deg H(x) \leq n-k-2$. *Then* $a_{n-1}^{k+1} \equiv 0 \pmod{m}$.

Proof. Denote $a := a_{n-1}$. By comparison of the coefficients, we find that

$$mc_{k-1} = a, \tag{2.6}$$

$$\binom{m}{2} c_{k-1}^2 + mc_{k-2} \in \mathbb{Z}. \tag{2.7}$$

From (2.6) and (2.7), it follows that

$$(m-1)a^2 + 2! \cdot m^2 c_{k-2} \in m\mathbb{Z}$$

and

$$2! \cdot m^2 c_{k-2} \equiv a^2 \pmod{m}.$$

We claim that

$$l! \cdot m^l c_{k-l} \equiv a^l \pmod{m} \qquad \text{for} \quad l = 1, 2, \ldots, k-1. \tag{2.8}$$

Consider the following system of equations

$$\begin{aligned} \alpha_0 \cdot k + \alpha_1 \cdot (k-1) + \cdots &= mk - l, \\ \alpha_0 + \alpha_1 + \cdots &= m, \\ \alpha_i \in \mathbb{Z}, \qquad \alpha_i &\geq 0. \end{aligned} \tag{2.9}$$

Let X denote the set of all solutions of the system (2.9). Then the coefficient with x^{n-l} on the right-hand side of (2.5) is equal to

$$\sum_{(\alpha_0,\alpha_1,\ldots)\in X} \frac{m!}{\prod \alpha_i!} c_{k-1}^{\alpha_1} c_{k-2}^{\alpha_2} \cdot \ldots .$$

The solutions of system (2.9) correspond to the solutions of system (2.1) from Lemma 1. Now we have that

$$\left(\sum_{\substack{(\alpha_1,\ldots,\alpha_l)\in Y \\ (\alpha_1,\ldots,\alpha_l)\neq(0,\ldots,0,1)}} \frac{m!}{\left(m-\sum_{i=1}^{l}\alpha_i\right)!\prod_{i=1}^{l}\alpha_i!} c_{k-1}^{\alpha_1} c_{k-2}^{\alpha_2} \cdots c_{k-l}^{\alpha_l} \right) + m c_{k-l} \tag{2.10}$$

is an integer. If $(\alpha_1,\ldots,\alpha_l)\neq(0,\ldots,0,1)$, then $\alpha_l = 0$ and, by induction hypothesis, the summands in (2.10) have the form

$$\frac{(m-1)!}{\left(m-\sum_{i=1}^{l}\alpha_i\right)!} \cdot \frac{a^l + mT}{\prod_{i=1}^{l}\alpha_i! \prod_{i=1}^{l}(i!)^{\alpha_i} \cdot m^{l-1}}$$

for an integer T. Multiplying by $l!\, m^{l-1}$, we obtain

$$\sum_{(\alpha_1,\ldots,\alpha_l)\neq(0,\ldots,0,1)} \frac{(m-1)!}{\left(m-\sum_{i=1}^{l}\alpha_i\right)!} \cdot \frac{l!a^l}{\prod_{i=1}^{l}\alpha_i! \prod_{i=1}^{l}(i!)^{\alpha_i}} + l!\, m^l c_{k-l} \in m\mathbb{Z}.$$

Indeed, $(m-1)!/(m-\sum_{i=1}^{l}\alpha_i)!$ is obviously an integer, and $l!/\prod_{i=1}^{l}\alpha_i! \prod_{i=1}^{l}(i!)^{\alpha_i}$ is also an integer since it is the number of all partitions of $\{1,\ldots,l\}$ in α_1 blocks of size 1, α_2 blocks of size $2,\ldots,\alpha_l$ blocks of size l. Now the congruence (2.8) follows directly from Lemma 1 and the fact that for $\alpha = (0,\ldots,0,1)\in Y$, it holds

$$\frac{(m-1)!}{\left(m-\sum_{i=1}^{l}\alpha_i\right)!} \cdot \frac{l!}{\prod_{i=1}^{l}\alpha_i! \prod_{i=1}^{l}(i!)^{\alpha_i}} = 1.$$

By considering the coefficients with x^{n-k}, we obtain

$$k!\, m^k c_0 + b m^{k-1} k! \equiv a^k \pmod{m}. \tag{2.11}$$

From the coefficient with $x^{n-(k+1)}$ (and writing formally $c_{-1} = 0$), we obtain

$$m \cdot c_{-1} + m(m-1)c_{k-1}c_0 + (\text{terms without } c_0) + (m-1)bc_{k-1} \in \mathbb{Z}.$$

Using (2.6) and (2.11), we get

$$(m-1)a\left(\frac{a^k}{k!\,m^k}-\frac{b}{m}+\frac{ms}{k!\,m^k}\right)+(\text{terms without } c_0)+\frac{(m-1)ab}{m}\in\mathbb{Z}$$

for an integer s. Multiplying this relation by $(k+1)!m^k$, the sum of terms without c_0, multiplied by $(k+1)!m^k$, is congruent to ka^{k+1} modulo m. Indeed, the corresponding sum from Lemma 1 does not contain solutions $(0,\dots,0,1),(1,0,\dots,0,1,0)\in Y$, and the contribution of these solutions is

$$\frac{(m-1)!}{(m-1)!}\cdot\frac{(k+1)!}{(k-1)!}+\frac{(m-1)!}{(m-2)!}\cdot\frac{(k+1)!}{k!}\equiv -k \pmod m.$$

Hence, we obtain

$$(k+1)(m-1)a^{k+1}+ka^{k+1}\equiv 0 \pmod m,$$

which clearly implies $a^{k+1}\equiv 0 \pmod m$. ∎

Remark 1. Let us note that the assumption (2.5) of Theorem 1 implies that in the Laurent series expansion of $(f(x))^{1/m}$ (in powers of $1/x$) the coefficient of $1/x$ vanishes. On the other hand, from $(f(x))^{1/m}=x^k(1+a_{n-1}x^{-1}+\cdots)^{1/m}$ one can show that this coefficient has the form $a_{n-1}^{k+1}+Am/(1+Bm)$, for integers A,B, which leads to the conclusion that $a_{n-1}^{k+1}\equiv 0 \pmod m$.

Corollary 1. *If $f(x)=x^n+a_{n-1}x^{n-1}+\cdots\in\mathbb{Z}[x]$ is a monic polynomial satisfying $\gcd(a_{n-1},n)=1$, then f is indecomposable.*

In [4], the first two authors considered also the decomposability problem for even and odd polynomials. They have shown that a decomposition of an odd polynomial is equivalent to a decomposition of the form $G\circ H$, where G and H are odd polynomials. On the other hand, let $f=g\circ h$ be a decomposition of an even polynomial f. Then h is an even polynomial, or $g=G\circ L$ and $h=L^{-1}\circ H$, where G is even, H is odd and L is a linear polynomial. Furthermore, they proved the following indecomposability results:

(i) Let $f(x)=x^n+a_{n-2}x^{n-2}+\cdots\in\mathbb{Z}[x]$ be an odd polynomial. If $\gcd(a_{n-2},n)=1$, then f is indecomposable.

(ii) Let $f(x)=x^{2n}+a_{n-2}x^{2n-2}+\cdots\in\mathbb{Z}[x]$ be an even polynomial and define $g(x)=f(\sqrt{x})$. Assume that $\gcd(a_{n-2},n)=1$. Then every decomposition of f is equivalent to one of the following decompositions: $f=g(x^2), f=(xp(x^2))^2$. The second case appears if and only if $g(x)=xp(x)^2$ for some polynomial $p(x)\in\mathbb{Z}[x]$.

Here we state generalizations of these results, which can be proved in the same manner as Theorem 1. Alternatively, one can use the Laurent series expansions, as in Remark 1. The only difference is that if the polynomials f and h from Theorem 3 are even, then the assumption of Theorem 3 implies vanishing of the coefficient of $1/x^2$, instead of the coefficient of $1/x$.

Theorem 2. *Let* $f(x) = x^n + a_{n-2}x^{n-2} + \cdots + a_1 x \in \mathbb{Z}[x]$ *be an odd polynomial. Assume that*

$$f(x) = (h(x))^m + H(x),$$

with $h(x), H(x) \in \mathbb{C}[x]$, $\deg h(x) = k$ *and* $\deg H(x) \leq n - k - 3$. *Then the polynomial* $h(x)$ *is odd and it holds* $a_{n-2}^{(k+1)/2} \equiv 0 \pmod{m}$.

Theorem 3. *Let* $f(x) = x^n + a_{n-2}x^{n-2} + \cdots + a_0 \in \mathbb{Z}[x]$ *be an even polynomial. Assume that*

$$f(x) = (h(x))^m + H(x),$$

with $h(x), H(x) \in \mathbb{C}[x]$, $\deg h(x) = k \geq 1$ *and* $\deg H(x) \leq n - k - 3$. *If* k *is odd, that the polynomial* $h(x)$ *is odd and* $a_{n-2}^{(k+1)/2} \equiv 0 \pmod{m}$, *and if* k *is even, then* $h(x)$ *is even and* $a_{n-2}^{(k+2)/2} \equiv 0 \pmod{m}$.

As a corollary of Theorems 1–3, we obtain a new proof of the characterization of all decompositions of Fibonacci polynomials.

Corollary 2. (*i*) *The Fibonacci polynomials* F_n *cannot be represented in the form* $F_n(x) = (h(x))^m + H(x)$, *where* $m \geq 2$ *and* $\deg h + \deg H \leq n - 4$.

(*ii*) *The polynomial* F_n *is indecomposable for even* n, *while for odd* n *the only decomposition* (*up to equivalence*) *of* F_n *is* $F_n(x) = f_n(x^2)$, *where* $f_n(x) = F_n(\sqrt{x})$.

Proof. The first statement of the corollary follows from Theorems 2 and 3. Indeed, if $F_n(x) = (h(x))^m + H(x)$, where $m \geq 2$ and $\deg h + \deg H \leq n - 4$, then $\deg H \leq \deg F_n - \deg h - 3$. Therefore, we may apply Theorems 2 and 3 to the polynomials $F_n(x) = x^{n-1} + (n-2)x^{n-3} + \cdots$. We get $(n-2)^{\lfloor (\deg h+1)/2 \rfloor} \equiv 0 \pmod{m}$, for a divisor $m > 1$ of $n - 1$, which is a contradiction.

Let us prove statement (ii). Assume first that n is even. Then F_n is an odd polynomial. If F_n is decomposable, then by [4, Lemma 2] we have $F_n = K \circ L$, where K and L are odd monic polynomials and $\deg K, \deg L \geq 3$. Hence, $F_n(x) = (L(x))^m + H(x)$, where $m = \deg K$

and $\deg H \leq (m-2)\deg L = \deg F_n - 2\deg L \leq n - \deg L - 4$, a contradiction.

Assume now that n is odd. Then F_n is an even polynomial. Let $F_n = K \circ L$ be a decomposition of F_n, where K and L are monic polynomials. By [4, Lemma 3], we may assume that L is an odd or even polynomial. If L is odd and $\deg L \geq 3$, then K is even, and we have $F_n(x) = (L(x))^{\deg K} + H(x)$, where $\deg H \leq n - \deg L - 4$, and we get a contradiction, as before.

Assume finally that L is an even polynomial, and define $l(x) = L(\sqrt{x})$. Now we have $f_n = K \circ l$. Let $K(x) = x^m + bx^{m-1} + \cdots$. If $\deg l \geq 2$, then $f_n(x) = (l(x))^m + b(l(x))^{m-1} + H(x)$, where $\deg H \leq (m-2)\deg l = \deg f_n - 2\deg l \leq \deg f_n - \deg l - 2$. Thus, we may apply Theorem 1, and we obtain a contradiction. Hence, we conclude that $\deg l = 1$ and $\deg L = 2$, and this implies that the decomposition $F_n = K \circ L$ is equivalent to $F_n(x) = f_n(x^2)$. ■

References

[1] BILU, YU., BRINDZA, B., KIRSCHENHOFER, P., PINTÉR, Á., TICHY, R. F. (2002) Diophantine equations and Bernoulli polynomials (with an appendix by A. Schinzel). Compositio Math. **131**: 173–188

[2] BILU, YU., STOLL, TH., TICHY, R. F. (2000) Octahedrons with equally many lattice points. Period. Math. Hungar. **40**: 229–238

[3] BILU, YU., TICHY, R. F. (2000) The Diophantine equation $f(x) = g(y)$. Acta Arith. **95**: 261–288

[4] DUJELLA, A., GUSIĆ, I. (to appear) Indecomposability of polynomials and related Diophantine equations. Quart. J. Math. Oxford

[5] DUJELLA, A., TICHY, R. F. (2001) Diophantine equations for second order recursive sequences of polynomials. Quart. J. Math. Oxford Ser. (2) **52**: 161–169

[6] GRAHAM, R. L., KNUTH, D. E., PATASHNIK, O. (1994) Concrete Mathematics. Addison-Wesley, Reading

[7] KIRSCHENHOFER, P., PFEIFFER, O. (2003) Diophantine equations between polynomials obeying second order recurrences. Period. Math. Hungar. **47**: 119–134

[8] SCHINZEL, A. (1982) Selected Topics on Polynomials. University of Michigan Press, Ann Arbor, MI

[9] SCHINZEL, A. (2000) Polynomials with Special Regard to Reducibility. In: Encyclopedia of Mathematics and Its Applications, Vol. 77. Cambridge Univ. Press, Cambridge, MA

[10] STOLL, TH., TICHY, R. F. (2003) Diophantine equations for classical continuous orthogonal polynomials. Indag. Math. **14**: 263–274

[11] STOLL, TH., TICHY, R. F. (2004) Diophantine equations involving general Meixner and Krawtchouk polynomials. Quaestiones Mathematicae **27**: 1–11

[12] STOLL, TH., TICHY, R. F. (submitted) Diophantine equations for Morgan-Voyce and other modified orthogonal polynomials

Authors' addresses: Andrej Dujella, Department of Mathematics, University of Zagreb, Bijenička cesta 30, 10000 Zagreb, Croatia. E-Mail: duje@math.hr; Ivica

Gusić, Faculty of Chemical Engineering and Technology, University of Zagreb, Marulićev trg 19, 10000 Zagreb, Croatia. E-Mail: igusic@fkit.hr; Prof. Dr. Robert F. Tichy, Institut für Mathematik, Technische Universität Graz, Steyrergasse 30, 8010 Graz, Austria. E-Mail: tichy@tugraz.at.