On the indecomposability of polynomials

Andrej Dujella, Ivica Gusić and Robert F. Tichy

Abstract

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

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]).

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, 11, 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*

$$\begin{aligned} \alpha_1 \cdot 1 + \alpha_2 \cdot 2 + \cdots + \alpha_l \cdot l &= l \\ 1 \leq \alpha_1 + \alpha_2 + \cdots + \alpha_l &\leq m. \end{aligned} \tag{2.1}$$

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, Section 6.1]) that the Stirling numbers satisfy the recurrence

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

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 formula (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* $h(x) = x^k + c_{k-1}x^{k-1} + \cdots + c_0 \in \mathbb{Q}[x]$, $k \geq 2$. *Assume that*

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

with $b \in \mathbb{Q}$, $H(x) \in \mathbb{Q}[x]$ *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

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

Consider the following system of equations

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

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

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

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

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

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

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

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

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

Indeed, $\frac{(m-1)!}{(m-\sum_{i=1}^{l}\alpha_i)!}$ is obviously an integer, and $\frac{l!}{\prod_{i=1}^{l}\alpha_i! \prod_{i=1}^{l}(i!)^{\alpha_i}}$ 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, ... , α_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

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

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 $(0, \ldots, 0, 1), (1, 0, \ldots, 0, 1, 0) \in Y$, 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 $a^{k+1} \equiv 0 \pmod{m}$. ∎

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: $f = g(x^2)$, $f = \big(xp(x^2)\big)^2$. 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.

THEOREM **2** *Let* $f(x) = x^n + a_{n-2}x^{n-2} + \cdots + a_1x \in \mathbb{Z}[x]$ *and* $h(x) = x^k + c_{k-2}x^{k-2} + \cdots + c_1x \in \mathbb{Q}[x]$, $k \geq 3$ *be odd polynomials. Assume that*

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

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

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

References

[1] Yu. Bilu, B. Brindza, P. Kirschenhofer, Á. Pintér and R. F. Tichy, *Diophantine equations and Bernoulli polynomials*, (with an appendix by A. Schinzel), Compositio Math. **131** (2002), 173–188.

[2] Yu. Bilu, Th. Stoll and R. F. Tichy, *Octahedrons with equally many lattice points*, Period. Math. Hungar. **40** (2000), 229–238.

[3] Yu. Bilu and R. F. Tichy, *The Diophantine equation $f(x) = g(y)$*, Acta Arith. **95** (2000), 261–288.

[4] A. Dujella and I. Gusić, *Indecomposability of polynomials and related Diophantine equations*, submitted.

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

[6] R. L. Graham, D. E. Knuth and O. Patashnik, Concrete Mathematics, Addison-Wesley, Reading, 1994.

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

[8] A. Schinzel, *Selected Topics on Polynomials*, University of Michigan Press, 1982.

[9] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia of Mathematics and its Applications **77**, Cambridge Univ. Press, 2000.

[10] Th. Stoll and R. F. Tichy, *Diophantine equations for classical continuous orthogonal polynomials*, Indag. Math. **14** (2003), 263–274.

[11] Th. Stoll and R. F. Tichy, *Diophantine equations involving general Meixner and Krawtchouk polynomials*, Quaestiones Mathematicae **27** (2004), 1 - 11.

[12] Th. Stoll and R. F. Tichy, *Diophantine equations for Morgan-Voyce and other modified orthogonal polynomials*, submitted.

Andrej Dujella
Department of Mathematics
University of Zagreb
Bijenička cesta 30
10000 Zagreb, Croatia
E-mail address: duje@math.hr

Ivica Gusić
Faculty of Chemical Engineering and Technology
University of Zagreb
Marulićev trg 19
10000 Zagreb, Croatia
E-mail address: igusic@fkit.hr

Robert F. Tichy
Institut für Mathematik
TU Graz
Steyrergasse 30
A-8010 Graz, Austria.
E-mail address: tichy@tugraz.at