GLASNIK MATEMATIČKI
Vol. 55(75)(2020), 13 – 27

DIOPHANTINE EQUATIONS CONNECTED TO THE KOMORNIK POLYNOMIALS

András Bazsó, Attila Bérczes, Ondřej Kolouch, István Pink and Jan Šustek

Hungarian Academy of Sciences, Hungary, University of Debrecen, Hungary and University of Ostrava, Czech Republic

Abstract. We investigate the power and polynomial values of the polynomials $P_n(X) = \prod_{k=0}^{n}\big(X^{2\cdot 3^k} - X^{3^k} - 1\big)$ for $n \in \mathbb{N}$. We prove various ineffective and effective finiteness results. In the case $0 \le n \le 3$, we determine all pairs x, y of integers such that $P_n(x) = y^2$ or $P_n(x) = y^3$.

1. Introduction

For $n = 0, 1, 2, \ldots$, let $A_n(X) = X^{2\cdot 3^n} - X^{3^n} - 1$. The polynomials

$$P_n(X) = \prod_{k=0}^{n} A_k(X) = \prod_{k=0}^{n}\big(X^{2\cdot 3^k} - X^{3^k} - 1\big).$$

were introduced by Komornik, Pedicini and Pethő ([10]), who – in a more general form – used them to show the existence of common expansions of real numbers in more than two non-integer bases if one of the bases is fixed. Thus we call these polynomials Komornik polynomials. See [10] for details. The

2020 *Mathematics Subject Classification.* 11D41, 11B83.

Key words and phrases. Diophantine equations, decomposition, polynomial values.

The research of the authors was supported in part by the Hungarian Academy of Sciences, by the NKFIH grants ANN130909, K115479 and K128088, the project EFOP-3.6.1-16-2016-00022 co-financed by the European Union and the European Social Fund, and by the project 17-02804S of the Czech science foundation.

first few such polynomials are:

$$\begin{aligned} P_0(X) &= X^2 - X - 1, \\ P_1(X) &= X^8 - X^7 - X^6 - X^5 + X^4 + X^3 - X^2 + X + 1, \\ P_2(X) &= X^{26} - X^{25} - X^{24} - X^{23} + X^{22} + X^{21} - X^{20} + X^{19} + X^{18} \\ &\quad - X^{17} + X^{16} + X^{15} + X^{14} - X^{13} - X^{12} + X^{11} - X^{10} \\ &\quad - X^9 - X^8 + X^7 + X^6 + X^5 - X^4 - X^3 + X^2 - X - 1. \end{aligned}$$

During the 23rd Czech and Slovak International Conference on Number Theory Pethő asked about the finiteness of solutions of the Diophantine equation

$$P_n(x) = P_m(y), \tag{1.1}$$

in $x, y \in \mathbb{Z}$. In the present paper we investigate a generalization of equation (1.1), and as a consequence we give a positive answer to the question of Pethő. Similar problems have been investigated in the past for many other families of polynomials. For example Péter, Pintér, and Schinzel ([16]) and Schinzel ([18]) considered such equations in trinomials, Stoll and Tichy ([19]) investigated the problem for general Meixner and Krawtchouk polynomials, Bilu, Brindza, Kirschenhofer, Pintér and Tichy ([4]) for Bernoulli polynomials, Kreso ([12, 11]) for lacunary polynomials, and Dubickas and Kreso ([7]) for truncated binomial powers. Rakaczki ([17]) investigated polynomial values of power sums, Kulkarni and Sury ([13]) polynomial values of products of consecutive numbers, Bazsó, Bérczes, Hajdu and Luca ([2]) polynomial values of sums of products of consecutive integers and Bazsó ([1]) polynomial values of alternate power sums.

2. New results

First we consider polynomial values of the polynomials $P_n(X)$. More precisely, for a polynomial $g(X) \in \mathbb{Q}[X]$, we consider the Diophantine equation

$$P_n(x) = g(y), \tag{2.1}$$

in integers x, y. Using the general finiteness criterion of Bilu and Tichy ([5]) we prove the following result.

Theorem 2.1. *For $n \geq 1$ and $\deg g \geq 3$, equation (2.1) has only finitely many integer solutions x, y unless we have*

(i) *$g(X) = P_n(h(X))$, where $h \in \mathbb{Q}[X]$ with $\deg h \geq 1$.*
(ii) *$g(X) = \gamma(\delta(X)^\ell)$, where $\ell = \deg g$ and $\gamma, \delta \in \mathbb{Q}[X]$ with $\deg \gamma = \deg \delta = 1$.*

We note that, since the criterion ([5]) mentioned above is ineffective, our Theorems 2.1 and 2.2 are also ineffective. We also remark that in case (i) of Theorem 2.1 there are infinitely many solutions to equation (2.1), meanwhile it is not clear whether excluding case (ii) is necessary or not for the finiteness of the solutions of (2.1).

In the special case $g(Y) = P_m(Y)$, we can derive a finiteness result from the above theorem, giving a complete answer to the question of Pethő.

THEOREM 2.2. *For $m > n \geq 1$, the equation*

$$P_n(x) = P_m(y), \tag{2.2}$$

has only finitely many integer solutions x, y.

Another interesting special case of equation (2.1) is when $g(Y) = Y^n$. For this special case it is again possible to deduce a complete, however ineffective finiteness result from Theorem 2.1, however, using the theory of superelliptic equations we can even obtain the below effective finiteness result.

THEOREM 2.3. *Let $m \geq 2$ and $n \geq 0$ be integers and put $d := 3^{n+1} - 1$. Then the equation*

$$P_n(x) = y^m, \qquad \text{in } x, y \in \mathbb{Z} \tag{2.3}$$

has only finitely many solutions, and these solutions fulfil the following inequalities:

1. *if $m = 2$ then*
$$\max\{|x|, |y|\} \leq \exp\left\{(4d)^{212d^4}\right\};$$
2. *if $m \geq 3$ then*
$$\max\{|x|, |y|\} \leq \exp\left\{(6d)^{14m^3d^3}\right\};$$
3. *if m is also considered to be unknown, and $y \neq \pm 1$ then*
$$m \leq \left(10d^2\right)^{40d}.$$

In principal the above result gives a naive algorithm to completely solve the equations in question. However, the bounds are too large to enumerate all the solutions up to the given bounds, even for moderate values of n.

Now we shall consider the equation

$$P_n(x) = y^2, \qquad \text{in } x, y \in \mathbb{Z}, \tag{2.4}$$

and solve it completely for some values of n.

REMARK 2.4. Clearly for every n the pairs $(x, y) = (-1, \pm 1)$ are solutions of equation (2.4). Moreover if n is odd then $(x, y) = (0, \pm 1)$ and $(x, y) = (1, \pm 1)$ are also solutions. In the sequel we shall refer to these solutions as *trivial solutions*.

THEOREM 2.5. *Let n be a non-negative integer. Then we have the following statements:*

1. *If $n=0$ then the only integer solutions of the equation (2.4) are*

$$(x,y)=(-1,\pm 1) \quad \textit{and} \quad (x,y)=(2,\pm 1).$$

2. *If $1 \le n \le 3$ then (2.4) has only trivial solutions.*

Remark 2.6. We were able to prove also for $1 \le n \le 5$ that (2.4) has only trivial solutions, using a similar technique, but the proof is much more technical.

Open Problem 1. *Is it true that for all $n \ge 1$ equation (2.4) has only trivial solutions?*

Similarly to equation (2.4) we also consider

$$P_n(x)=y^3, \qquad \text{in } x,y\in\mathbb{Z}, \tag{2.5}$$

and solve it completely for some values of n.

Remark 2.7. Clearly for every n the pair $(x,y)=(-1,1)$ is a solution of equation (2.5). Moreover if n is odd then $(x,y)=(0,1)$ and $(x,y)=(1,1)$ and if n is even then $(x,y)=(0,-1)$ and $(x,y)=(1,-1)$ are also solutions. In the sequel we shall refer to these solutions as *trivial solutions*.

Theorem 2.8. *Let n be a non-negative integer. Then we have the following statements:*

1. *If $n=0$ then the only integer solutions of the equation (2.5) are*

$$(x,y)\in\{(1,-1),(2,1),(-36,11),(-1,1),(-1,0),(37,11)\}.$$

2. *If $1 \le n \le 3$ then (2.5) has only trivial solutions.*

3. Auxiliary results

In this section, we present some earlier results needed to prove our theorems. First, we recall the finiteness criterion of Bilu and Tichy ([5]). To do this, we need to define five kinds of so-called standard pairs of polynomials.

Let α,β,δ be nonzero rational numbers, $\mu,\nu,q>0$ and $r\ge 0$ be integers, and let $v(X)\in\mathbb{Q}[X]$ be a nonzero polynomial (which may be constant). Denote by $D_\mu(X,\delta)$ the μ-th Dickson polynomial, given by

$$D_\mu(X,\delta)=\sum_{i=0}^{\lfloor \mu/2\rfloor} d_{\mu,i}X^{\mu-2i} \quad \text{with} \quad d_{\mu,i}=\frac{\mu}{\mu-i}\binom{\mu-i}{i}(-\delta)^i.$$

Note that these polynomials have only terms with the same parity of exponents. For other properties of Dickson polynomials, we refer to [14].

Two polynomials $F(X)$ and $G(X)$ are said to form a *standard pair over* $\mathbb{Q}$ if one of the ordered pairs $(F(X),G(X))$ or $(G(X),F(X))$ belongs to the list collected in Table 1.

Now we state a special case of the main result of [5], which will be crucial in the proof of Theorem 2.1.

kind	standard pair	parameter restrictions
first	$(X^q, \alpha X^r v(X)^q)$	$0 \leq r < q, \gcd(r, q) = 1,$ $r + \deg v > 0$
second	$(X^2, (\alpha X^2 + \beta)v(X)^2)$	$-$
third	$(D_\mu(X, \alpha^\nu), D_\nu(X, \alpha^\mu))$	$\gcd(\mu, \nu) = 1$
fourth	$(\alpha^{\frac{-\mu}{2}} D_\mu(X, \alpha), -\beta^{\frac{-\nu}{2}} D_\nu(X, \beta))$	$\gcd(\mu, \nu) = 2$
fifth	$((\alpha X^2 - 1)^3, 3X^4 - 4X^3)$	$-$

TABLE 1. Standard pairs

LEMMA 3.1. *Let $f(X), g(X) \in \mathbb{Q}[X]$ be nonconstant polynomials such that the equation $f(x) = g(y)$ has infinitely many solutions in integers x, y. Then $f = \varphi \circ F \circ \lambda$ and $g = \varphi \circ G \circ \kappa$, where $\lambda(X), \kappa(X) \in \mathbb{Q}[X]$ are linear polynomials, $\varphi(X) \in \mathbb{Q}[X]$, and $F(X), G(X)$ form a standard pair over $\mathbb{Q}$.*

The polynomial $f \in \mathbb{C}[X]$ is called *indecomposable* over $\mathbb{C}$ if $f = g \circ h$ for $g, h \in \mathbb{C}[X]$ implies $\deg g = 1$ or $\deg h = 1$.

The next statement is due to Dujella and Gusić ([6]).

LEMMA 3.2. *Let $f(X) = X^n + aX^{n-1} + \cdots \in \mathbb{Z}[X]$. If $\gcd(a, n) = 1$, then f is indecomposable over $\mathbb{C}$.*

4. PROPERTIES OF THE KOMORNIK POLYNOMIALS $P_n(X)$

4.1. *Basic properties of $P_n(X)$.*

LEMMA 4.1. *The polynomials $P_n(X)$ have the following properties:*

1. *The degree of $P_m(X)$ is $3^{n+1} - 1$;*
2. *$P_n(X)$ consists of 3^{n+1} monomials;*
3. *All the coefficients of $P_n(X)$ are ± 1;*
4. *All the complex roots of $P_n(X)$ are simple.*

PROOF. To prove Lemma 4.1 it is enough to see the fact, that $P_n(X)$ is the product of the trinomials $A_0(X), \ldots, A_n(X)$. Clearly, the degree of the polynomial will be

$$2 + 2 \cdot 3 + 2 \cdot 3^2 + \cdots + 2 \cdot 3^n = 3^{n+1} - 1$$

and each monomial of the product $A_0(X) \cdot \ldots \cdot A_n(X)$ will have the form

$$\pm X^{\sum_{i=0}^{n} d_i \cdot 3^i},$$

where $d_i \in \{0, 1, 2\}$. This shows that in the exponent of all monomials arising from multiplying the trinomials $A_0(X), \ldots, A_n(X)$ we get the digit expansion in base 3 of a number from the range $0, \ldots, 3^{n+1} - 1$. Each number from this range is obtained as an exponent exactly once, so there are no terms with the same exponent to collect, i.e. there will be 3^{n+1} monomials each having coefficient ± 1.

Let $\varphi := \frac{1+\sqrt{5}}{2}$ denote the golden section. Then clearly the roots of the polynomial $P_n(X)$ are φ, $\psi := \frac{-1}{\varphi}$ and all the complex k^{th} roots of φ and ψ for $k = 3, 3^2, \dots, 3^n$. These roots are pairwise distinct. Indeed, $|\varphi| > 1$ and $|\psi| < 1$, so no k^{th} root φ can be equal to any l^{th} root of ψ. Further, for $k \neq l$ no k^{th} root of φ can be equal to any l^{th} root of φ and no k^{th} root of ψ can be equal to any l^{th} root of ψ since their absolute values are different. Finally, for given k the k pieces of k^{th} roots of both φ and ψ are pairwise distinct. So indeed, all the complex roots of $P_n(X)$ are simple. ∎

4.2. *Divisibility properties of $A_k(X)$.* In this subsection we shall investigate the greatest common divisor of the values of the factors $A_k(X)$ of the Komornik polynomials $P_n(X)$ at integer values of X. Clearly, for every $k, l \geq 0$ the polynomials A_k satisfy the polynomial identity

$$A_{l+k}(X) = A_l\big(X^{3^k}\big). \tag{4.1}$$

Let Φ_s denote the s-th Fibonacci number, defined by

$$\begin{aligned} &\Phi_0 := 0, \quad \Phi_1 := 1 \\ &\Phi_{s+2} := \Phi_s + \Phi_{s+1} \end{aligned} \tag{4.2}$$

and extend the definition to negative indices by the formula

$$\Phi_{-s} = (-1)^{s+1}\Phi_s. \tag{4.3}$$

Clearly by this definition the recurrence relation (4.2) is satisfied for all $s \in \mathbb{Z}$.

LEMMA 4.2. *Let m be an odd natural number. Then we have the polynomial identity*

$$\begin{aligned} \left(\sum_{i=0}^{m-1} \Phi_{-1-i} X^i - \sum_{i=0}^{2m-1} \Phi_{m-1-i} X^i\right)&(X^2 - X - 1) \\ &+ (\Phi_m X - \Phi_{m+1})(X^{2m} - X^m - 1) = \Phi_{m+1} + \Phi_{m-1} - 1. \end{aligned}$$

PROOF. Using the recurrence relation (4.2) of the Fibonacci numbers, a simple computation shows that

$$\left(\sum_{i=0}^{m-1} \Phi_{-1-i} X^i\right)(X^2 - X - 1) = \Phi_{-m} X^{m+1} + \Phi_{-1-m} X^m - 1 \tag{4.4}$$

and

$$\left(\sum_{i=0}^{2m-1} \Phi_{m-1-i} X^i\right)(X^2 - X - 1) = \Phi_{-m} X^{2m+1} + \Phi_{-1-m} X^{2m} - \Phi_m X - \Phi_{m-1}. \tag{4.5}$$

Finally, using (4.4) and (4.5) along with (4.3) we obtain for every odd number m that

$$\begin{aligned}
&\left(\sum_{i=0}^{m-1}\Phi_{-1-i}X^i-\sum_{i=0}^{2m-1}\Phi_{m-1-i}X^i\right)(X^2-X-1)\\
&\quad+(\Phi_mX-\Phi_{m+1})(X^{2m}-X^m-1)\\
&=(\Phi_{-m}X^{m+1}+\Phi_{-1-m}X^m-1)\\
&\quad-(\Phi_{-m}X^{2m+1}+\Phi_{-1-m}X^{2m}-\Phi_mX-\Phi_{m-1})\\
&\quad+(\Phi_mX^{2m+1}-\Phi_{m+1}X^{2m}-\Phi_mX^{m+1}+\Phi_{m+1}X^m-\Phi_mX+\Phi_{m+1})\\
&=(\Phi_mX^{m+1}-\Phi_{m+1}X^m-1)-(\Phi_mX^{2m+1}-\Phi_{m+1}X^{2m}-\Phi_mX-\Phi_{m-1})\\
&\quad+(\Phi_mX^{2m+1}-\Phi_{m+1}X^{2m}-\Phi_mX^{m+1}+\Phi_{m+1}X^m-\Phi_mX+\Phi_{m+1})\\
&=\Phi_{m+1}+\Phi_{m-1}-1.
\end{aligned}$$

□

For non-negative integers k we define the numbers

$$R_k=\Phi_{3^k+1}+\Phi_{3^k-1}-1.$$

Lemma 4.3. *For every $k,l\ge 0$ and every $x\in\mathbb{Z}$ the numbers $A_l(x)$ and $A_{l+k}(x)$ satisfy*

$$\gcd\bigl(A_l(x),A_{l+k}(x)\bigr)\bigm| R_k.$$

Proof. Lemma 4.2 implies that we have the polynomial identity

$$\pi_k(X)A_0(X)+\rho_k(X)A_k(X)=R_k$$

for suitable polynomials $\pi_k,\rho_k\in\mathbb{Z}[X]$, proving that for every $t\in\mathbb{Z}$ we have

$$\gcd\bigl(A_0(t),A_k(t)\bigr)\bigm| R_k.$$

Finally, by equation (4.1), for every $x\in\mathbb{Z}$, we have

$$\gcd\bigl(A_l(x),A_{l+k}(x)\bigr)=\gcd\bigl(A_0(x^{3^l}),A_k(x^{3^l})\bigr)\bigm| R_k,$$

which concludes the proof of our lemma. □

Lemma 4.4. *For every $k\ge 0$ and every $x\in\mathbb{Z}$ we have*

$$\gcd\bigl(A_k(x),A_{k+1}(x)\bigr)=1.$$

Proof. Since $R_1=3$, thus Lemma 4.3 implies for every $x\in\mathbb{Z}$ that

$$\gcd\bigl(A_0(x),A_1(x)\bigr)\bigm| 3.$$

Working modulo 3 we see that $A_0(0)\equiv A_0(1)\equiv 2 \pmod 3$ and $A_0(2)\equiv 1 \pmod 3$. Hence $A_0(x)$ is never divisible by 3 and for every $x\in\mathbb{Z}$ we have $\gcd(A_0(x),A_1(x))=1$. Again, we use (4.1) to finish the proof. □

Lemma 4.5. *For every $k \geq 0$ and every $x \in \mathbb{Z}$ we have*

$$\gcd\bigl(A_k(x), A_{k+2}(x)\bigr) = \begin{cases} 5 & \textit{if} \quad k \equiv 0 \pmod 2 \quad \textit{and} \quad x \equiv 3 \pmod 5, \\ 5 & \textit{if} \quad k \equiv 1 \pmod 2 \quad \textit{and} \quad x \equiv 2 \pmod 5, \\ 1 & \textit{else.} \end{cases}$$

Proof. Since $R_2 = 3 \cdot 5^2$, Lemma 4.3 implies for every $x \in \mathbb{Z}$ that

$$\gcd\bigl(A_0(x), A_2(x)\bigr) \bigm| 3 \cdot 5^2.$$

From the proof of Lemma 4.4 we know that $A_0(x)$ is never divisible by 3. Working modulo 5 we see that $A_0(x) \equiv A_2(x) \equiv 0 \pmod 5$ if and only if $x \equiv 3 \pmod 5$. Working modulo 5^2 we see that $A_0(x) \equiv 0 \pmod{5^2}$ never occurs. Hence

$$\gcd\bigl(A_0(x), A_2(x)\bigr) = \begin{cases} 5 & \text{if } x \equiv 3 \pmod 5, \\ 1 & \text{if } x \not\equiv 3 \pmod 5. \end{cases}$$

From this, (4.1) and the fact that $x^3 \equiv 3 \pmod 5$ if and only if $x \equiv 2 \pmod 5$ we obtain that

$$\gcd\bigl(A_1(x), A_3(x)\bigr) = \begin{cases} 5 & \text{if } x \equiv 2 \pmod 5, \\ 1 & \text{if } x \not\equiv 2 \pmod 5. \end{cases}$$

For every $x \in \mathbb{Z}$ we have $x^{3^2} \equiv x \pmod 5$. Then (4.1) implies for every non-negative integer s that

$$\gcd\bigl(A_{s+2}(x), A_{s+4}(x)\bigr) = \gcd\bigl(A_s(x), A_{s+2}(x)\bigr)$$

and the result follows by induction. □

4.3. *Square values of $A_k(X)$.*

Lemma 4.6. *Let $k \geq 0$. Then the only integer solutions of the equation*

$$A_k(x) = y^2$$

are $(x, y) = (-1, \pm 1)$ and $(x, y) = (2, \pm 1)$ for $k = 0$ and $(x, y) = (-1, \pm 1)$ for $k \geq 1$.

Proof. First we prove the statement for $k = 0$, so we consider the equation

$$A_0(x) = x^2 - x - 1 = y^2 \quad \text{in } x, y \in \mathbb{Z}. \tag{4.6}$$

We shall split the argument into three cases.

1. If $x < -1$ then

$$x^2 < x^2 - x - 1 < x^2 - 2x + 1 = (x-1)^2.$$

Hence if (x, y) is a solution of (4.6) then $y \in \,]x-1, x[$, a contradiction.

2. If $x > 2$ then
$$(x-1)^2 = x^2 - 2x + 1 < x^2 - x - 1 < x^2.$$
Hence if (x, y) is a solution of (4.6) then $y \in]x-1, x[$, a contradiction.
3. For $x = -1, 0, 1, 2$ one can easily check that for $x = -1$ and for $x = 2$ we have a solution and that for $x = 0$ and for $x = 1$ we do not have a solution.

Now using equation (4.1) we see that $A_k(x) = A_0(x^{3^k})$, thus our equation yields that $x^{3^k} \in \{-1, 2\}$, hence for $k \geq 1$ we get $x = -1$. ∎

4.4. *Cube values of $A_k(X)$.*

Lemma 4.7. *Let $k \geq 0$. Then the integer solutions of the equation*
$$A_k(x) = y^3$$
are $(x, y) \in \{(1, -1), (0, -1), (2, 1), (-1, 1), (37, 11), (-36, 11)\}$ *for* $k = 0$ *and* $(x, y) \in \{(1, -1), (-1, 1), (0, -1)\}$ *for* $k \geq 1$.

Proof. First we prove the statement for $k = 0$, so we consider the equation
$$x^2 - x - 1 = y^3 \quad \text{in } x, y \in \mathbb{Z}. \tag{4.7}$$
By multiplying both sides of (4.7) by 64, we obtain
$$(8x - 4)^2 - 80 = (4y)^3, \tag{4.8}$$
which is a Mordell equation $Y^2 - k = X^3$ with $k = 80, X = 4y$ and $Y = 8x - 4$. By e.g. [15], the integer solutions X, Y of (4.8) are
$$(X, Y) \in \{(-4, \pm 4), (1, \pm 9), (4, \pm 12), (44, \pm 292)\},$$
whence, in (4.7), we obtain
$$(x, y) \in \{(1, -1), (0, -1), (2, 1), (-1, 1), (37, 11), (-36, 11)\},$$
proving the statement for $k = 0$. For more on Mordell's equation, see [9].

Now using equation (4.1) we see that $A_k(x) = A_0(x^{3^k})$, thus our equation yields that $x^{3^k} \in \{1, 2, -36, -1, 0, 37\}$, hence for $k \geq 1$ we get $x \in \{1, -1, 0\}$ proving the statement for $k \geq 1$. ∎

4.5. *Indecomposability of $P_n(X)$.* Using Lemma 3.2, we prove the following.

Lemma 4.8. *The polynomial $P_n(X)$ is indecomposable over $\mathbb{C}$ for $n \geq 0$.*

Proof. For every $n \geq 0$, it is easy to see from the definition of $P_n(X)$ that the coefficient of $X^{\deg P_n(X) - 1} = X^{3^{n+1} - 2}$ in $P_n(X)$ is equal to -1. Hence we obviously have $\gcd(3^{n+1} - 1, -1) = 1$, which, by Lemma 3.2, implies that $P_n(X)$ is indecomposable over $\mathbb{C}$. ∎

4.6. *On the form of the polynomial $P_n(c_1X+c_0)$.* In the present subsection we start to investigate whether a linear transformation of $P_n(X)$ can be a linear transformation of a polynomial belonging to some standard pair of the first, third or fourth kind. Let $c_1, c_0, e_1, e_0 \in \mathbb{Q}$ with $c_1 \neq 0$ and $e_1 \neq 0$. Put

$$P_n(c_1X+c_0) = a_qX^q + a_{q-1}X^{q-1} + \ldots + a_1X + a_0,$$

where $q = 3^{n+1}-1$. We observe the following:

$$a_q = c_1^q,$$

$$a_{q-1} = c_1^{q-1}\left(qc_0 - 1\right), \tag{4.9}$$

$$a_{q-2} = c_1^{q-2}\left(\binom{q}{2}c_0^2 - (q-1)c_0 - 1\right), \tag{4.10}$$

$$a_{q-3} = c_1^{q-3}\left(\binom{q}{3}c_0^3 - \binom{q-1}{2}c_0^2 - (q-2)c_0 - 1\right). \tag{4.11}$$

Lemma 4.9. *The polynomial $P_n(c_1X+c_0)$ with $c_1 \neq 0$ is not of the form $e_1X^q + e_0$ with $q \geq 3$.*

Proof. Suppose that $P_n(c_1X+c_0) = e_1X^q + e_0$ with some fixed $q \geq 3$. Then clearly $e_1 \neq 0$ and $q = 3^{n+1}-1$. Comparing the coefficients of X^{q-1} on both sides, by (4.9) we get $c_0 = 1/q$. Comparing now the coefficients of X^{q-2} we obtain by (4.10) that

$$0 = \frac{q(q-1)}{2}c_0^2 - (q-1)c_0 - 1 = \frac{q(q-1)}{2q^2} - \frac{q-1}{q} - 1 = \frac{1}{2q} - \frac{3}{2} \leq -\frac{4}{3},$$

a contradiction. ∎

Lemma 4.10. *The polynomial $P_n(c_1X+c_0)$ with $c_1 \neq 0$ is not of the form*

$$e_1D_\nu(X,\delta) + e_0,$$

where $D_\nu(X,\delta)$ is the ν-th Dickson polynomial with $\nu \geq 3$ and $\delta \in \mathbb{Q}\setminus\{0\}$.

Proof. Suppose that $P_n(c_1X+c_0) = e_1D_\nu(X,\delta) + e_0$ with some fixed $\nu \geq 3$ and $\delta \in \mathbb{Q}\setminus\{0\}$. Then we have $e_1 \neq 0$ and $\nu = 3^{n+1}-1$. In particular, $n \geq 1$. Comparing the coefficients of $X^{\nu-1}$ on both sides, by (4.9) we obtain $c_0 = 1/\nu$. Comparing now the coefficients of $X^{\nu-3}$ we obtain by (4.11) and by $c_1 \neq 0$ that

$$\begin{aligned}
0 &= \frac{\nu(\nu-1)(\nu-2)}{6}c_0^3 - \frac{(\nu-1)(\nu-2)}{2}c_0^2 - (\nu-2)c_0 - 1 \\
&= \frac{\nu(\nu-1)(\nu-2)}{6\nu^3} - \frac{(\nu-1)(\nu-2)}{2\nu^2} - \frac{\nu-2}{\nu} - 1 \\
&= -\frac{(\nu-1)(7\nu-2)}{3\nu^2} < 0,
\end{aligned}$$

a contradiction. ∎

5. Proofs of the Theorems

Proof of Theorem 2.1. Let $n \geq 1$ and $g(X) \in \mathbb{Q}[X]$ be a polynomial with $\deg g \geq 3$. Suppose that equation (2.1) has infinitely many solutions in integers x, y. Then by Lemma 3.1, there exist $\lambda(X), \kappa(X), \varphi(X) \in \mathbb{Q}[X]$ with $\deg \lambda = \deg \kappa = 1$ such that

$$P_n(X) = \varphi(F(\lambda(X))) \quad \text{and} \quad g(X) = \varphi(G(\kappa(X))), \tag{5.1}$$

where $F(X), G(X)$ form a standard pair over $\mathbb{Q}$. By Lemma 4.8, (5.1) implies that

$$\deg \varphi \in \left\{1, 3^{n+1} - 1\right\}.$$

Assume that $\deg \varphi = 3^{n+1} - 1$. Then, by (5.1), we observe that $\deg F = 1$. Thus $P_n(X) = \varphi(t(X))$, where $t(X) = F(\lambda(X)) \in \mathbb{Q}[X]$ is a polynomial with $\deg t = 1$. Clearly, we have $t^{-1} \in \mathbb{Q}[X]$ and $\deg t^{-1} = 1$. By (5.1), we obtain

$$P_n(t^{-1}(X)) = \varphi(t(t^{-1}(X))) = \varphi(X).$$

Hence,

$$g(X) = \varphi(G(\kappa(X))) = P_n(t^{-1}(G(\kappa(X)))) = P_n(h(X)),$$

where $h(X) = t^{-1}(G(\kappa(X)))$. So, if in this case equation (2.1) has infinitely many solutions, then $g(X)$ is of the form $P_n(h(X))$, where $h \in \mathbb{Q}[X]$ with $\deg h \geq 1$.

In the sequel we assume $\deg \varphi = 1$. Then there exist $\varphi_0, \varphi_1 \in \mathbb{Q}$ with $\varphi_1 \neq 0$ such that $\varphi(X) = \varphi_1 X + \varphi_0$. We study now the five kinds of standard pairs. In view of our assumptions $n \geq 1$, i.e., $\deg F = \deg P_n \geq 8$ and $\deg G = \deg g \geq 3$, it follows that $F(X)$ and $G(X)$ cannot form a standard pair of the second or fifth kind.

If the the polynomials $F(X)$ and $G(X)$ form a standard pair of the third or fourth kind, we then have

$$P_n(\lambda^{-1}(X)) = \varphi(F(X)) = e_1 D_\nu(X, \delta) + e_0$$

for some $e_0 \in \mathbb{Q}$ and $e_1, \delta \in \mathbb{Q} \setminus \{0\}$, contradicting Lemma 4.10, since $\nu = \deg F \geq 8$.

Finally, if in (5.1), $F(X)$ and $G(X)$ form a standard pair of the first kind, then we have either

(a) $P_n(\lambda^{-1}(X)) = \varphi(F(X)) = \varphi_1 X^q + \varphi_0$, or
(b) $P_n(\lambda^{-1}(X)) = \varphi(F(X)) = \varphi_1 \alpha X^r v(X)^q + \varphi_0$, where $0 \leq r < q$, $(r, q) = 1$ and $r + \deg v > 0$.

Case (a) is impossible by Lemma 4.9 since $q = \deg F \geq 8$.

In case (b), we have $G(X) = X^q$ and $g(X) = \varphi_1 \kappa(X)^q + \varphi_0$. Then we have $q = \deg g$ and we are led to (ii), which completes the proof. ∎

Proof of Theorem 2.2. Let $m > n \geq 1$ and suppose that equation (2.2) has infinitely many solutions in integers x, y. In view of Theorem 2.1, it suffices to prove that the polynomial $P_m(X)$ is neither of the form as in (i) nor as in (ii).

If $P_m(X) = P_n(h(X))$ for some nonconstant polynomial $h \in \mathbb{Q}[X]$, then Lemma 4.8 implies that $\deg h = 1$ and thus $\deg P_m = \deg(P_n \circ h)$, which is a contradiction since $m > n$.

Let $P_m(X) = \gamma(\delta(X)^\ell)$, for some linear polynomials $\gamma, \delta \in \mathbb{Q}[X]$ and a positive integer ℓ. Since $m \geq 1$, i.e. $\ell = \deg P_m \geq 8$, we get a contradiction by Lemma 4.9 which finishes the proof. □

Proof of Theorem 2.3. This is a simple consequence of [3, Theorems 2.2, 2.1 and 2.3]. Indeed, by Lemma 4.1 all the roots of $P_n(X)$ are simple roots, thus we may apply the above mentioned results of [3] for the equation (2.3) in the special case $f = P_n$, $K = \mathbb{Q}$, $\mathcal{O}_S = \mathbb{Z}$ and $b = 1$. Using the notation of [3], since $b = 1$, thus $\hat{h}$ is the logarithmic height of $f = P_n$, and since all the coefficients of P_n are ± 1, thus $\hat{h} = 0$. Further, since we are searching for rational integer solutions and also $P_n(X) \in \mathbb{Z}[X]$, thus we have $s = 1$, $D_K = 1$ and $Q_S = 1$. Further, by Lemma 4.1 the degree of P_n is $d = 3^{n+1} - 1$. Thus the statements of our Theorem 2.3 follow from [3, Theorems 2.2, 2.1 and 2.3]. □

Proof of Theorem 2.5. To prove part 1 of the theorem in fact we have to solve the Diophantine equation

$$A_0(x) = y^2,$$

in integers x, y and this case is covered by Lemma 4.6.

To prove part 2 for $n = 1$ we have to solve the equation

$$A_0(x)A_1(x) = y^2 \quad \text{in integers } x, y. \tag{5.2}$$

Suppose that $(x, y) \in \mathbb{Z}^2$ is a nontrivial solution. Hence $|x| \geq 2$ and

$$A_1(x) > 0. \tag{5.3}$$

Then (5.2), (5.3) and Lemma 4.4 imply that there must be an integer z such that $A_1(x) = z^2$. But Lemma 4.6 implies that this equation has no integer solution with $|x| > 1$.

To prove part 2 for $n = 2$ we have to solve the equation

$$A_0(x)A_1(x)A_2(x) = y^2 \quad \text{in integers } x, y. \tag{5.4}$$

Suppose that $(x, y) \in \mathbb{Z}^2$ is a nontrivial solution. One easily checks that $x \neq 0$ and $x \neq 1$. Hence $|x| \geq 2$ and we have (5.3). Lemma 4.4 implies that

$$\gcd\big(A_1(x), A_0(x)\big) = \gcd\big(A_1(x), A_2(x)\big) = 1.$$

Hence $\gcd\big(A_1(x), A_0(x)A_2(x)\big) = 1$ and (5.3) and (5.4) imply that there must be an integer z such that $A_1(x) = z^2$, a contradiction with Lemma 4.6.

Finally to prove part 2 for $n = 3$ we have to solve the equation

$$A_0(x)A_1(x)A_2(x)A_3(x) = y^2 \quad \text{in integers } x, y. \tag{5.5}$$

Suppose that $(x, y) \in \mathbb{Z}^2$ is a nontrivial solution. Then $|x| \geq 2$ and hence

$$A_1(x) > 0 \quad \text{and} \quad A_2(x) > 0. \tag{5.6}$$

Now we consider two cases. First, if $x \equiv 3 \pmod 5$ then Lemma 4.4 and Lemma 4.5 imply that

$$\gcd\bigl(A_1(x), A_0(x)\bigr) = \gcd\bigl(A_1(x), A_2(x)\bigr) = \gcd\bigl(A_1(x), A_3(x)\bigr) = 1.$$

Hence $\gcd\bigl(A_1(x), A_0(x)A_2(x)A_3(x)\bigr) = 1$ and (5.5) and (5.6) imply that there must be an integer z such that $A_1(x) = z^2$, a contradiction with Lemma 4.6. Secondly, if $x \not\equiv 3 \pmod 5$ then Lemma 4.4 and Lemma 4.5 imply that

$$\gcd\bigl(A_2(x), A_0(x)\bigr) = \gcd\bigl(A_2(x), A_1(x)\bigr) = \gcd\bigl(A_2(x), A_3(x)\bigr) = 1$$

which in turn proves that $\gcd\bigl(A_2(x), A_0(x)A_1(x)A_3(x)\bigr) = 1$, so now there must be an integer z such that $A_2(x) = z^2$, again a contradiction. $\square$

Proof of Theorem 2.8. We shall follow the proof of Theorem 2.5. Part 1 is covered by Lemma 4.7.

To prove part 2 for $n = 1$ we have to solve the equation

$$A_0(x)A_1(x) = y^3 \quad \text{in integers } x, y. \tag{5.7}$$

Suppose that $(x, y) \in \mathbb{Z}^2$ is a nontrivial solution. Hence $|x| \geq 2$ and

$$A_1(x) > 0. \tag{5.8}$$

Then (5.7), (5.8) and Lemma 4.4 imply that there must be an integer z such that $A_1(x) = z^3$. But Lemma 4.7 implies that this equation has no integer solution with $|x| > 1$.

To prove part 2 for $n = 2$ we have to solve the equation

$$A_0(x)A_1(x)A_2(x) = y^3 \quad \text{in integers } x, y. \tag{5.9}$$

Suppose that $(x, y) \in \mathbb{Z}^2$ is a nontrivial solution. Hence $|x| \geq 2$ and we have (5.8). Lemma 4.4 implies that

$$\gcd\bigl(A_1(x), A_0(x)\bigr) = \gcd\bigl(A_1(x), A_2(x)\bigr) = 1.$$

Hence $\gcd\bigl(A_1(x), A_0(x)A_2(x)\bigr) = 1$ and (5.8) and (5.9) imply that there must be an integer z such that $A_1(x) = z^3$, which together with $|x| \geq 2$ contradicts Lemma 4.7.

Finally, to prove part 2 for $n = 3$ we have to solve the equation

$$A_0(x)A_1(x)A_2(x)A_3(x) = y^3 \quad \text{in integers } x, y. \tag{5.10}$$

Suppose that $(x, y) \in \mathbb{Z}^2$ is a nontrivial solution. Then $|x| \geq 2$ and hence

$$A_1(x) > 0 \quad \text{and} \quad A_2(x) > 0. \tag{5.11}$$

Then Lemma 4.4 and Lemma 4.5 imply that

$$\gcd\bigl(A_1(x), A_0(x)\bigr) = \gcd\bigl(A_1(x), A_2(x)\bigr) = 1$$

and $\gcd\bigl(A_1(x), A_3(x)\bigr) \mid 5$. Hence $\gcd\bigl(A_1(x), A_0(x)A_2(x)A_3(x)\bigr) \mid 5$ and (5.10) and (5.11) imply that there must be an integer z such that $A_1(x) = z^3$ or $A_1(x) = 5z^3$.

Now $A_1(x) = z^3$ and $|x| \geq 2$ is in contradiction with Lemma 4.7. Secondly, $A_1(x) = 5z^3$ means

$$(x^3)^2 - x^3 - 1 = 5z^3.$$

Multiplying by 25 and using the notation $u = 5x^3$ and $v = 5z$ this is equivalent to the elliptic curve

$$u^2 - 5u - 25 = v^3.$$

Using Magma we determined the integer points on this curve, which are $(v, u) \in \{(-1, -3), (-1, 8), (5, -10), (5, 15)\}$, which together with $u = 5x^3$, $x \in \mathbb{Z}$ gives a contradiction. So we only have the trivial solutions, as stated in part 2 of Theorem 2.8. $\square$

References

[1] A. Bazsó, *Polynomial values of (alternating) power sums,* Acta Math. Hungar. **146** (2015), 202–219.

[2] A. Bazsó, A. Bérczes, L. Hajdu and F. Luca, *Polynomial values of sums of products of consecutive integers,* Monatsh. Math. **187** (2018), 21–34.

[3] A. Bérczes, J.-H. Evertse and K. Győry, *Effective results for hyper- and superelliptic equations over number fields,* Publ. Math. Debrecen **82** (2013), 727–756.

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

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

[6] A. Dujella and I. Gusić, *Indecomposability of polynomials and related Diophantine equations,* Q. J. Math. **57** (2006), 193–201.

[7] A. Dubickas and D. Kreso, *Diophantine equations with truncated binomial polynomials,* Indag. Math. (N.S.) **27** (2016), 392–405.

[8] P. Erdős and J. Surányi, Topics in the theory of numbers. (Translated from the second Hungarian edition by Barry Guiduli.) Undergraduate Texts in Mathematics, Springer-Verlag, New York, 2003.

[9] J. Gebel, A. Pethő and H. G. Zimmer, *On Mordell's equation,* Compositio Math. **110** (1998), 335–367.

[10] V. Komornik, M. Pedicini and A. Pethő, *Multiple common expansions in non-integer bases,* Acta Sci. Math. (Szeged) **83** (2017), 51–60.

[11] D. Kreso, *On common values of lacunary polynomials at integer points,* New York J. Math. **21** (2015), 987–1001.

[12] D. Kreso, *Diophantine equations in separated variables and lacunary polynomials,* Int. J. Number Theory, **13** (2017), 2055–2074.

[13] M. Kulkarni and B. Sury, *On the Diophantine equation $x(x+1)(x+2)\dots(x+(m-1)) = g(y)$*, Indag. Math. (N.S.) **14** (2003), 35–44.

[14] R. Lidl, G. Mullen and G. Turnwald, Dickson polynomials, Pitman Monographs and Surveys in Pure and Applied Mathematics **65**, Longman Scientific & Technical, Harlow, 1993.

[15] H. London and R. Finkelstein, On Mordell's equation $y^2 - k = x^3$, Bowling Green State university, Bowling Green, OH, 1973.

[16] Gy. Péter, A. Pintér and A. Schinzel, *On equal values of trinomials,* Monatsh. Math. **162** (2011), 313–320.

[17] Cs. Rakaczki, *On the Diophantine equation $S_m(x) = g(y)$,* Publ. Math. Debrecen **65** (2004), 439–460.

[18] A. Schinzel, *Equal values of trinomials revisited,* Tr. Mat. Inst. Steklova **276** (2012), 255–261.

[19] T. Stoll and R. F. Tichy, *Diophantine equations involving general Meixner and Krawtchouk polynomials,* Quaest. Math. **28** (2005), 105–115.

A. Bazsó
Institute of Mathematics
MTA-DE Research Group "Equations Functions and Curves"
Hungarian Academy of Sciences and University of Debrecen
P.O. Box 400, H-4002 Debrecen
Hungary
E-mail: bazsoa@science.unideb.hu

A. Bérczes
Institute of Mathematics
University of Debrecen
P.O. Box 400, H-4002 Debrecen
Hungary
E-mail: berczesa@science.unideb.hu

O. Kolouch
Department of Mathematics
University of Ostrava
30. dubna 22, Ostrava, 701 03
Czech Republic
E-mail: ondrej.kolouch@osu.cz

I. Pink
Institute of Mathematics
University of Debrecen
P.O. Box 400, H-4002 Debrecen
Hungary
E-mail: pinki@science.unideb.hu

J. Šustek
Department of Mathematics
University of Ostrava
30. dubna 22, Ostrava, 701 03
Czech Republic
E-mail: jan.sustek@osu.cz

Received: 26.4.2019.
Revised: 10.8.2019.