DIOPHANTINE EQUATIONS WITH TRUNCATED BINOMIAL POLYNOMIALS

ARTŪRAS DUBICKAS AND DIJANA KRESO

ABSTRACT. For positive integers $k \le n$ let $P_{n,k}(x) := \sum_{j=0}^{k} \binom{n}{j} x^j$ be the binomial expansion of $(1+x)^n$ truncated at the kth stage. In this paper we show the finiteness of solutions of Diophantine equations of type $P_{n,k}(x) = P_{m,l}(y)$ in $x, y \in \mathbb{Z}$ under assumption of irreducibility of truncated binomial polynomials $P_{n-1,k-1}(x)$ and $P_{m-1,l-1}(x)$. Although the irreducibility of $P_{n,k}(x)$ has been studied by several authors, in general, this problem is still open. In addition, we give some results about the possible ways to write $P_{n,k}(x)$ as a functional composition of two lower degree polynomials.

1. Introduction and main results

For positive integers $k \le n$ put

$$P_{n,k}(x) := \sum_{j=0}^{k} \binom{n}{j} x^j = \binom{n}{0} + \binom{n}{1} x + \binom{n}{2} x^2 + \cdots + \binom{n}{k} x^k.$$

The polynomial $P_{n,k}(x)$ is said to be a *truncated binomial expansion* (*polynomial*) at the kth stage. We study Diophantine equations of type

$$P_{n,k}(x) = P_{m,l}(y) \quad \text{with} \quad n, k, m, l \in \mathbb{N},\ k \le n-1,\ l \le m-1. \tag{1.1}$$

We prove that the equation (1.1) has only finitely many integer solutions under certain reasonable assumptions. The main results are deduced from a general finiteness criterion for the Diophantine equation $f(x) = g(y)$ established by Bilu and Tichy in [2]. The proof requires several auxiliary results about the possible ways to write a truncated binomial expansion as a functional composition of two lower degree polynomials, as the above mentioned theorem of Bilu and Tichy essentially says that the equation of type $f(x) = g(y)$ has only finitely many solutions in integers x, y, unless the polynomials $f(x)$ and $g(x)$ can be written as a functional composition of

2010 *Mathematics Subject Classification.* 11D41, 12D10, 12E10.
Key words and phrases. Truncated binomial expansion, Dickson polynomial, Diophantine equations.

some lower degree polynomials in a prescribed way. Factorization of polynomials under the operation of functional composition, i.e. "polynomial decomposition" was first studied by Ritt [13], and subsequently investigated and applied by many other authors; see, for instance, [2, 6, 9, 12, 15, 18, 20].

Our interest in the equation (1.1) has arisen from our considerations of decomposition properties of truncated binomial expansions. Note that $P'_{n,k}(x) = nP_{n-1,k-1}(x)$, so if $P_{n,k}(x) = g(h(x))$, where $g(x), h(x) \in \mathbb{Q}[x]$ satisfy $\deg g > 1$ and $\deg h > 1$, then

$$nP_{n-1,k-1}(x) = P'_{n,k}(x) = g'(h(x))h'(x),$$

and, consequently, the polynomial $P_{n-1,k-1}(x)$ is reducible over $\mathbb{Q}$. The question of irreducibility of truncated binomial expansions first appeared in [14]. It was studied by Filaseta, Kumchev and Pasechnik [8], and subsequently by Khanduja, Khassa and Laishram [10]. There are indications that the polynomials $P_{n,k}(x)$ are irreducible for all pairs $k, n \in \mathbb{N}$ satisfying $k \leq n-2$, although this problem is still far from being solved. It is known that $P_{n,k}(x)$ are irreducible for $n \leq 100$ and $k \leq n-2$, see [8]. It is easy to see that $P_{n,k}(x)$ is irreducible for $k = 2$, since in this case the discriminant of the polynomial is negative, so that it has two complex roots. It is also known that $P_{n,k}(x)$ are irreducible for all $k, n \in \mathbb{N}$ satisfying $2k \leq n < (k+1)^3$, see [10]. Furthermore, as it was shown in [8] for any fixed integer $k \geq 3$ there exists an integer $n_0(k)$ such that $P_{n,k}(x)$ is irreducible for every $n \geq n_0$. Finally, in the same paper it was proved that if n is prime, then $P_{n,k}(x)$ is irreducible for each k in the range $1 \leq k \leq n-1$.

In this paper we prove the following.

Theorem 1.1. *Let $n, k, m, l \in \mathbb{N}$ be such that $2 \leq k \leq n-1, 2 \leq l \leq m-1$ and $k \neq l$. If $P_{n-1,k-1}(x)$ and $P_{m-1,l-1}(x)$ are irreducible, then the equation $P_{n,k}(x) = P_{m,l}(y)$ has at most finitely many integer solutions (x, y).*

Note that the truncated binomial expansion at the last stage, i.e. when $k = n-1$, takes the form $P_{n,n-1}(x) = (x+1)^n - x^n$. If n is a composite integer, then $P_{n,n-1}(x)$ is clearly reducible. If $n = p$ is a prime, then the polynomial $P_{n,n-1}(x) = P_{p,p-1}(x)$ is irreducible, by the Eisenstein criterion applied to the reciprocal polynomial $x^{p-1}P_{p,p-1}(1/x)$. As an auxiliary result we show that if n is even, then $P_{n,n-1}(x)$ cannot be written in the form

$$P_{n,n-1}(x) = g(x) \circ h(x) = g(h(x))$$

with $g(x), h(x) \in \mathbb{C}[x]$ and $\deg g > 1$, $\deg h > 1$. We further show that if n is odd, then essentially the only way to write $P_{n,n-1}(x)$ as a functional composition of polynomials of lower degree is the following: write $n = 2n'+1$ and $\omega_j = \exp(2\pi ij/n)$, $j = 1, 2, \ldots, n$, so that $\omega_n = 1$ and $\omega_{n-j} = \overline{\omega_j}$ for all $j = 1, 2, \ldots, n'$. Then

$$P_{n,n-1}(x) = \left(\prod_{j=1}^{n'} ((2 - \omega_j - \overline{\omega_j})x + 1) \right) \circ (x^2 + x).$$

Using these results we will prove the following.

Theorem 1.2. *For any positive integers $n > m \geq 3$ there are only finitely many integer solutions x, y of the equation*

$$(1+x)^n - x^n = (1+y)^m - y^m. \tag{1.2}$$

In Section 2 we recall some classical results on polynomial decomposition and present new ones on the possible decompositions of truncated binomial expansions and give some auxiliary results on the location of roots of $P_{n,k}(x)$. We show that $P_{n,k}(x)$ is indecomposable, i.e. not representable as a functional composition of lower degree polynomials, not only when $P_{n-1,k-1}(x)$ is irreducible, but also when for any two distinct roots of $P_{n-1,k-1}(x)$, say ζ and ξ, we have $\zeta^k \neq \xi^k$. Using the latter approach we will resolve the question of possible decompositions of $P_{n,k}(x)$ in the case $k = n-1$, which is our main tool in proving Theorem 1.2. The existence of such roots and the irreducibility of $P_{n-1,k-1}(x)$ with $k < n-1$ seem to be two independent questions, both of which remain generally open. Some results on polynomials which have two roots whose quotient is a root of unity can be found in [5, 16, 19].

In order to prove Theorem 1.1 and Theorem 1.2 we combine several of our auxiliary results together with the main result of [2] which we recall in Section 3. One of the difficulties is to describe all possibilities when the polynomial $P_{n,k}(x)$ is representable by linear transformation of a so-called Dickson polynomial given by

$$D_k(x, \gamma) = \sum_{j=0}^{\lfloor k/2 \rfloor} \frac{k}{k-j} \binom{k-j}{j} (-1)^j \gamma^j x^{k-2j}. \tag{1.3}$$

We shall prove slightly more than we need, namely, the following lemma.

Lemma 1.3. *For any integers $n > k \geq 3$ there do not exist $a, b, u, v \in \mathbb{R}$ and $c \geq 0$ for which the identity*

$$P_{n,k}(x) = aD_k(ux + v, c) + b \tag{1.4}$$

holds for all $x \in \mathbb{R}$. Furthermore, if $n > k \geq 4$, then (1.4) holds for some $a, b, u, v \in \mathbb{R}$ and $c < 0$ if and only if $(n, k) = (5, 4)$ and $v \neq 0$, $u = 2v$, $a = 5/(16v^4)$, $c = -v^2/2$, $b = -3/32$.

The proof of this lemma will be given in Section 4. In Section 5 we will complete the proof of Theorem 1.2. Finally, in Section 6 we prove Theorem 1.1 for $k, l \geq 3$ under assumption of indecomposability of $P_{n,k}(x)$ and $P_{m,l}(x)$ which is weaker than the assumption of irreducibility of $P_{n-1,k-1}(x)$ and $P_{m-1,l-1}(x)$ in Theorem 1.1. The case $m = 3$ of Theorem 1.2 and the case $l = 2$ (or $k = 2$) of Theorem 1.1 can be made effective and to that end we use Baker's theorem. These two cases are treated by Lemma 3.3 (see Section 3) and at the end of Section 6, respectively.

2. Functional decomposition

A polynomial $f(x) \in \mathbb{C}[x]$ with $\deg f > 1$ is called *indecomposable* (over $\mathbb{C}$) if it cannot be written as the composition $f(x) = g(x) \circ h(x) = g(h(x))$ with $g(x), h(x) \in \mathbb{C}[x]$ such that $\deg g > 1$ and $\deg h > 1$. Otherwise, $f(x)$ is said to be decomposable. Any representation of $f(x)$ as a functional composition of polynomials of degree greater than 1 is called a decomposition of $f(x)$. It follows by induction that any polynomial $f(x)$ with $\deg f > 1$ can be written as a composition of indecomposable polynomials. Such an expression of $f(x)$ is said to be a *complete decomposition* of $f(x)$.

Ritt [13] proved that any complete decomposition of $f(x)$ can be obtained from any other via finitely many steps, where each step consists of replacing two adjacent indecomposables by two others with the same composition. Ritt then solved the functional equation $a(b(x)) = c(d(x))$ in indecomposable polynomials $a(x), b(x), c(x), d(x) \in \mathbb{C}[x]$, and in this way completely described the extent of nonuniqueness of the "prime" factorization of polynomials with complex coefficients with respect to functional composition. For more on the topic of functional decomposition we refer to [15, Chap. 1] and [20]. We will make use of the following two results that belong to the classical theory of polynomial decomposition.

Proposition 2.1. *If $f(x) \in \mathbb{Q}[x]$ is decomposable (over $\mathbb{C}$), then it can be written as the functional composition of two polynomials of degree at least 2 in $\mathbb{Q}[x]$.*

For the proof of Proposition 2.1 see [15, Chap. 1, Theorem 6, p. 20] or the paper [9].

Proposition 2.2. *Assume that $f(x) = g_1(x) \circ g_2(x) = h_1(x) \circ h_2(x)$ for some $f(x), g_1(x), h_1(x), g_2(x), h_2(x) \in \mathbb{C}[x]$ such that $\deg g_1 = \deg h_1$, and hence $\deg g_2 = \deg h_2$. Then there exists a linear polynomial $\ell(x) \in \mathbb{C}[x]$ such that $g_1(x) = h_1(\ell(x))$ and $g_2(x) = \ell^{(-1)}(x) \circ h_2(x)$, where $\ell^{(-1)}(x)$ denotes the inverse of $\ell(x)$ with respect to functional composition.*

The proof of Proposition 2.2 can be found in [20, Corollary 2.9]. The result was first proved by Ritt [13].

We next introduce the following quantity. For $f(x) \in \mathbb{C}[x]$ and $\gamma \in \mathbb{C}$ let

$$\delta(f, \gamma) = \deg \gcd(f(x) - \gamma, f'(x)). \tag{2.1}$$

We have the following lemma.

Lemma 2.3. *If $f(x) = g(h(x))$ with $\deg g > 1$, $\deg h > 1$, then there exists $\gamma \in \mathbb{C}$ such that $\delta(f, \gamma) = \deg \gcd(f(x) - \gamma, f'(x)) \geq \deg h$.*

Proof. If β is a root of $g'(x)$ (which exists, since by the condition of the lemma, $\deg g' \geq 1$) and $\gamma = g(\beta)$, then $h(x) - \beta$ divides both $f(x) - \gamma$ and $f'(x) = g'(h(x))h'(x)$. □

From Lemma 2.3 it follows that if $f(x) \in \mathbb{C}[x]$ is such that $\delta(f, \gamma) \leq 1$ for all $\gamma \in \mathbb{C}$, then $f(x)$ is indecomposable. This approach in proving indecomposability was first used, to the best of our knowledge, by Beukers, Shorey and Tijdeman [3] to prove that for an arbitrary integer $m \geq 1$ the polynomial $f(x) = x(x+1)(x+2)\cdots(x+m)$ is indecomposable. It was further used by Dujella and Tichy [6] to study possible decompositions of Chebyshev polynomials of the second kind, as well as by Stoll [18] to prove that certain classes of orthogonal polynomials are indecomposable.

In the sequel we focus on possible decompositions of the truncated binomial polynomial $P_{n,k}(x)$. First note that

$$P'_{n,k}(x) = nP_{n-1,k-1}(x) \tag{2.2}$$

and

$$P_{n,k}(x) - (x+1)\frac{P'_{n,k}(x)}{n} = \binom{n-1}{k}x^k. \tag{2.3}$$

The following lemma will be very useful later on.

Lemma 2.4. *Let $k, n \in \mathbb{N}$ be such that $k \le n-1$. Then all the roots of $P_{n,k}(x)$ are simple. Furthermore, $P_{n,k}(x)$ has exactly one real root if k is odd, and no real roots if k is even.*

Proof. It follows from (2.3) that $P_{n,k}(x)$ has only simple roots. If k is even and $P_{n,k}(x)$ (of degree k) has a real root, then it must have at least two real roots. Assume that $x_0 < x_1$ are two smallest real roots. Then $x_0 < x_1 < 0$ and $P_{n,k}(x) < 0$ for each $x \in (x_0, x_1)$. Hence there exists $x_2 \in (x_0, x_1)$ such that $P'_{n,k}(x_2) = 0$ (by Rolle's theorem), which together with (2.3) implies

$$0 < \binom{n-1}{k}x_2^k = P_{n,k}(x_2) < 0,$$

a contradiction. If k is odd, then $P_{n,k}(x)$ clearly must have a real root. Assume that $k > 1$ and that $P_{n,k}(x)$ has another real root. Let $x_0 < x_1$ be the smallest real roots of $P_{n,k}(x)$. Then $x_0 < x_1 < 0$ and $P_{n,k}(x) > 0$ for each $x \in (x_0, x_1)$. Thus, there exists $x_2 \in (x_0, x_1)$ such that $P'_{n,k}(x_2) = 0$, wherefrom by (2.3) we get

$$0 > \binom{n-1}{k}x_2^k = P_{n,k}(x_2) > 0,$$

a contradiction. □

Lemma 2.5. *Let $n, k \in \mathbb{N}$ be such that $2 \le k \le n-1$ and the polynomial $P_{n-1,k-1}(x)$ is either irreducible or it does not have two distinct roots ζ and ξ satisfying $\zeta^k = \xi^k$. Then $P_{n,k}(x)$ is indecomposable.*

Proof. Assume to the contrary that $P_{n,k}(x)$ is decomposable. Then, by Proposition 2.1, it follows that $P_{n,k}(x) = g(h(x))$ for some $g(x), h(x) \in \mathbb{Q}[x]$ with $\deg g > 1$, $\deg h > 1$. Hence $g'(h(x))h'(x) = P'_{n,k}(x) = nP_{n-1,k-1}(x)$, by (2.2), so $P_{n-1,k-1}(x)$ is reducible, a contradiction.

Furthermore, by Lemma 2.3, there exists $\gamma \in \mathbb{C}$ such that $\delta(P_{n,k}, \gamma) = \deg \gcd(P_{n,k}(x) - \gamma, P'_{n,k}(x)) \ge \deg h \ge 2$. Since $P'_{n,k}(x) = nP_{n-1,k-1}(x)$ has only simple roots (see (2.2) and Lemma 2.4), it follows that there exist two distinct roots of $P_{n-1,k-1}(x)$, say ζ and ξ, such that $\gamma = P_{n,k}(\zeta) = P_{n,k}(\xi)$.

Note that then from (2.3) it follows that

$$\gamma = \binom{n-1}{k}\zeta^k = \binom{n-1}{k}\xi^k.$$

This yields $\zeta^k = \xi^k$, contrary to the assumption of the lemma. □

Remark 2.6. Computations (based on the algorithm [19, Method 2, Sect. 4.1]) show that for $n \leq 100$ and $k \leq n-2$ there do not exist two distinct roots of $P_{n-1,k-1}(x)$, say ζ and ξ, satisfying $\zeta^k = \xi^k$. The same is true when $n \leq 100$, $k = n-1$ and n is even. However, when $k = n-1$ and n is odd, the computations suggest that such two roots of $P_{n-1,k-1}(x)$ always exist. This will be explained by Lemma 2.9 below. As we shall see, $P_{n,k}(x)$ is in that case decomposable (see Proposition 2.8). It seems very likely that for $n \geq k+2$ no two distinct roots ζ and ξ of $P_{n-1,k-1}(x)$ satisfying $\zeta^k = \xi^k$ exist. By the result of Ferguson [7], this can be shown for k even, but, unfortunately, under assumption of irreducibility of $P_{n-1,k-1}(x)$.

Corollary 2.7. *For $n, k \in \mathbb{N}$ satisfying $2 \leq k \leq n-1$ the polynomial $P_{n,k}(x)$ is indecomposable if any of the following holds:*

- $k+2 \leq n \leq 101$,
- $2k-1 \leq n \leq k^3$,
- *k is a prime,*
- *$n-1$ is prime.*

Furthermore, for any fixed integer $k \geq 2$, there exists an integer $n_0(k)$ such that $P_{n,k}(x)$ is indecomposable for every $n \geq n_0(k)$.

Proof. In [10] it is shown that $P_{n-1,k-1}(x)$ is irreducible for all $k, n \in \mathbb{N}$ such that $2(k-1) \leq n-1 < k^3$. In [8] the same was checked for $k+2 \leq n \leq 101$. This combined with Lemma 2.5 implies the first two statements of the corollary. Since $\deg P_{n,k}(x) = k$, it is clear that $P_{n,k}(x)$ is indecomposable when k is a prime. Finally, as it was shown in [8], $P_{n,k}(x)$ is irreducible when n is a prime and also when n is large enough for each fixed k. This implies the last two assertions of the corollary. □

In the sequel we will completely describe the possible decompositions of $P_{n,n-1}(x)$. Note that if n is a composite integer, then $P_{n,n-1}(x)$ is clearly reducible. When n is odd, then $P_{n,n-1}(x)$ is also decomposable. Indeed, write $n = 2n'+1$ and $\omega_j = \exp(2\pi ij/n)$, $j = 1, 2, \ldots, n$ so that $\omega_{2n'+1} = 1$,

$\omega_{n-j} = \overline{\omega_j}$ for all $j = 1, 2, \dots, n'$. Then

$$\begin{aligned}(x+1)^n - x^n &= \prod_{j=1}^{n'} (x + 1 - \omega_j x)\,(x + 1 - \overline{\omega_j} x) \\ &= \prod_{j=1}^{n'} \big((2 - \omega_j - \overline{\omega_j})(x^2 + x) + 1\big) \\ &= \left(\prod_{j=1}^{n'} ((2 - \omega_j - \overline{\omega_j})x + 1) \right) \circ (x^2 + x).\end{aligned}$$

This identity can be rewritten as

$$P_{n,n-1}(x) = \tilde{P}_{n,n-1}(x) \circ (x^2 + x), \tag{2.4}$$

where

$$\tilde{P}_{n,n-1}(x) := \prod_{j=1}^{n'} ((2 - \omega_j - \overline{\omega_j})x + 1) \tag{2.5}$$

and n', ω_j are defined as above.

Proposition 2.8. *If n is even, then $P_{n,n-1}(x)$ is indecomposable. If n is odd and $P_{n,n-1}(x) = g(h(x))$ with $g(x), h(x) \in \mathbb{C}[x]$ and $\deg g > 1$, $\deg h > 1$, then there exists a linear polynomial $\mu(x) \in \mathbb{C}[x]$ such that*

$$g(x) = \tilde{P}_{n,n-1}(x) \circ \mu(x), \quad h(x) = \mu^{(-1)}(x) \circ (x^2 + x)$$

where $\tilde{P}_{n,n-1}(x)$ is defined as in (2.5), and $\mu^{(-1)}(x)$ denotes the inverse of $\mu(x)$ with respect to functional composition.

In the proof of Proposition 2.8 we will use the following lemma.

Lemma 2.9. *For every integer $n \geq 3$ and for any complex number γ we have $\delta(P_{n,n-1}, \gamma) = \deg \gcd(P_{n,n-1}(x) - \gamma, P'_{n,n-1}(x)) \leq 2$. Moreover, for n even we have $\delta(P_{n,n-1}, \gamma) \leq 1$.*

Proof. Since the roots of $P'_{n,n-1}(x) = n((x+1)^{n-1} - x^{n-1})$ are all simple, we have $\delta(P_{n,n-1}, \gamma) = r$ iff there exist exactly r distinct roots of $(x+1)^{n-1} - x^{n-1}$, say $\zeta_1, \dots, \zeta_r$, for which $P_{n,n-1}(\zeta_1), \dots, P_{n,n-1}(\zeta_r)$ are all equal. Take two roots α and β of $(x+1)^{n-1} - x^{n-1}$ such that $P_{n,n-1}(\alpha) = P_{n,n-1}(\beta)$. The former implies that $(\alpha+1)^{n-1} = \alpha^{n-1}$ and $(\beta+1)^{n-1} = \beta^{n-1}$, and so the latter yields $\alpha^{n-1} = \beta^{n-1}$. Note that the roots of $(x+1)^{n-1} - x^{n-1}$ are

$$z_k = \frac{1}{\omega^k - 1}, \quad 1 \leq k \leq n-2, \text{ where } \omega = \exp\left(\frac{2\pi i}{n-1}\right),$$

all of which lie on the vertical line $\Re(z) = -1/2$. Then from $\alpha^{n-1} = \beta^{n-1}$ it follows that α and β are complex conjugates, since they are distinct but have equal absolute values. Thus, r cannot exceed 2, and so $\delta(P_{n,n-1}, \gamma) \le 2$.

If $\delta(P_{n,n-1}, \gamma) = 2$, then there exists $\alpha \in \mathbb{C}$ such that α and $\overline{\alpha}$ are roots of $(x+1)^{n-1} - x^{n-1}$ and $\alpha^{n-1} = \overline{\alpha}^{n-1}$. Let $\zeta = \alpha/\overline{\alpha}$, so that $\zeta^{n-1} = 1$. Then for some k in the range $1 \le k \le n-2$ we have

$$\zeta = \frac{\alpha}{\overline{\alpha}} = \frac{1 - \overline{\omega^k}}{1 - \omega^k} = -\overline{\omega^k}.$$

From $\omega^{n-1} = 1$ and $\zeta^{n-1} = 1$ it follows that $1 = (-1)^{n-1}$, so n is odd. □

Proof of Proposition 2.8. From Lemma 2.9 and Lemma 2.3 it follows that $P_{n,n-1}(x)$ is indecomposable for even n. Let n be odd. Assume that $P_{n,n-1}(x) = g(h(x))$, where $\deg g > 1$ and $\deg h > 1$. From Proposition 2.9 and Lemma 2.3 it follows that then necessarily $\deg h = 2$, and hence $\deg g = (n-1)/2$. From (2.4) it follows that $\tilde{P}_{n,n-1}(x) \circ (x^2 + x) = g(h(x))$. Proposition 2.2 completes the proof. □

3. Standard pairs and the case $m = 3$ of Theorem 1.2

We first recall the main result of [2]. We say that the equation $f(x) = g(y)$ has infinitely many *rational solutions with a bounded denominator* if there exists $\lambda \in \mathbb{N}$ such that $f(x) = g(y)$ has infinitely many solutions $x, y \in \mathbb{Q}$ that satisfy $\lambda x, \lambda y \in \mathbb{Z}$. Note that if the equation $f(x) = g(y)$ has only finitely many rational solutions with a bounded denominator, then it clearly has only finitely many integer solutions.

We further need to define five kinds of so-called *standard pairs* of polynomials. In what follows a and b are nonzero rational numbers, k and l are positive integers, $r \ge 0$ is an integer, $q(x) \in \mathbb{Q}[x]$ is a nonzero polynomial (which may be a constant) and $D_m(x, a)$ is the mth Dickson polynomial with parameter a, defined by the functional equation

$$D_m\left(x + \frac{a}{x}, a\right) := x^m + \left(\frac{a}{x}\right)^m. \tag{3.1}$$

It is well known that

$$D_k(x, c) = 2c^{k/2} T_k(x/2\sqrt{c}), \tag{3.2}$$

where $T_k(x) = \cos(k \arccos x)$ is the kth Chebyshev polynomial of the first kind. Another useful expression for Dickson polynomials is the formula (1.3)

given in Section 1. With this notation five standard pairs of polynomials over $\mathbb{Q}$ are listed in the following table.

kind	standard pair (or switched)	parameter restrictions
first	$(x^k, ax^r q(x)^k)$	$0 \le r < k, \gcd(r,k) = 1,\ r + \deg p > 0$
second	$(x^2, (ax^2+b)q(x)^2)$	none
third	$(D_k(x,a^l), D_l(x,a^k))$	$\gcd(k,l) = 1$
fourth	$(a^{-k/2}D_k(x,a), -b^{-l/2}D_l(x,b))$	$\gcd(k,l) = 2$
fifth	$((ax^2-1)^3, 3x^4-4x^3)$	none

Theorem 3.1 (Bilu and Tichy, [2]). *Let $f(x)$ and $g(x)$ be nonconstant polynomials in $\mathbb{Q}[x]$. Then the following assertions are equivalent.*

- *The equation $f(x) = g(y)$ has infinitely many rational solutions with a bounded denominator.*
- *We have*

$$f(x) = \phi\left(f_1\left(\lambda(x)\right)\right), \quad g(x) = \phi\left(g_1\left(\mu(x)\right)\right),$$

where $\lambda(x), \mu(x) \in \mathbb{Q}[x]$ are linear polynomials, $\phi(x) \in \mathbb{Q}[x]$, and $(f_1(x), g_1(x))$ is a standard pair over $\mathbb{Q}$ such that the equation $f_1(x) = g_1(y)$ has infinitely many rational solutions with a bounded denominator.

The proof of Theorem 3.1 relies on Siegel's classical theorem on integral points on curves, and is consequently ineffective. Theorem 3.1 will be our main tool in the sequel for proving Theorem 1.1 and Theorem 1.2.

We will use the following result of Baker [1] to show that the case $m = 3$ of Theorem 1.2 can be made effective Later, it will be also used to treat the "small case" of Theorem 1.1, i.e. the case $k = 2$ or $l = 2$. (The first ineffective proof of this statement was given by Siegel [17].)

Proposition 3.2. *Let $f(x) \in \mathbb{Q}[x]$ be a polynomial with at least three simple roots. Then all solutions of the equation $f(x) = y^2$ in integers x, y satisfy $\max\{|x|, |y|\} \le C$, where C is an effectively computable constant depending only on the coefficients of $f(x)$.*

Lemma 3.3. *For each $n \ge 4$ the equation $(1+x)^n - x^n = (1+y)^3 - y^3$ has only finitely many integer solutions.*

Proof. Rewrite the equation as $4(1+x)^n - 4x^n - 1 = 3(2y+1)^2$. By Proposition 3.2, it suffices to show that $f(x) = 4(1+x)^n - 4x^n - 1$ has at least three

simple roots. We will show that all the roots of $f(x)$ are simple. Assume to the contrary that there exists $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0$ and $f'(\alpha) = 0$. The latter implies that $(1+\alpha)^{n-1} = \alpha^{n-1}$, wherefrom as in the proof of Lemma 2.9, we obtain $\alpha = 1/(\omega^k - 1)$ for $\omega = \exp(2\pi i/(n-1))$ and some k in the range $1 \le k \le n-2$. Furthermore,

$$0 = f(\alpha) = 4\alpha^{n-1}\left((1+\alpha)\frac{(1+\alpha)^{n-1}}{\alpha^{n-1}} - \alpha\right) - 1 = 4\alpha^{n-1} - 1$$

yields $1/4 = \alpha^{n-1}$, so that

$$4 = \left(\frac{1}{\alpha}\right)^{n-1} = (\omega^k - 1)^{n-1} = \left(2i\omega^{k/2}\sin\frac{\pi k}{n-1}\right)^{n-1}. \tag{3.3}$$

By comparing the absolute values of both sides, we obtain

$$4 = \left(2\sin\frac{\pi k}{n-1}\right)^{n-1}, \quad \text{wherefrom } \sin\frac{\pi k}{n-1} = 2^{-(n-3)/(n-1)}.$$

For $n = 4$ and $n \ge 6$, the right hand side, $2^{-(n-3)/(n-1)}$, is an algebraic number which has a complex (nonreal) conjugate, whereas the left hand side, $\sin\frac{\pi k}{n-1}$, is a totally real algebraic number, a contradiction. Hence $n = 5$. Then the right hand side is $2^{-(n-3)/(n-1)} = 1/\sqrt{2}$, and one easily checks that this equality is possible for $k = 1$ and $k = 3$. However, by inserting $n = 5$ and $k \in \{1, 3\}$ into (3.3) we find that $1 = (i\omega^{k/2})^4 = \omega^{2k} = \exp(\pi i k) = (-1)^k$, a contradiction. □

We conclude this section with the following simple lemma which will serve us in the proofs of Theorems 1.1 and 1.2.

Lemma 3.4. *For integers $n > k \ge 3$ there do not exist $a, b, u, v \in \mathbb{R}$ and $h(x) \in \mathbb{R}[x]$ with a root of multiplicity at least 3 for which the identity $ah(ux+v) + b = P_{n,k}(x)$ holds for all $x \in \mathbb{R}$.*

Proof. Assume to the contrary that such $a, b, u, v \in \mathbb{R}$ and $h(x) \in \mathbb{R}[x]$ exist. Note that $a, u \neq 0$. By taking derivatives of both sides of the identity, we obtain $auh'(ux+v) = P'_{n,k}(x) = nP_{n-1,k-1}(x)$. By the assumption on $h(x)$, the polynomial on the left hand side has a zero of multiplicity at least 2, whereas, by Lemma 2.4, all the zeros of $P_{n-1,k-1}(x)$ are simple, a contradiction. □

4. Proof of Lemma 1.3

Recall that $D_k(x,c)$ denotes the kth Dickson polynomial with parameter c, defined by (1.3) and (3.1). Dickson polynomials appear in the table of standard pairs over $\mathbb{Q}$. We now prove Lemma 1.3.

Proof of Lemma 1.3. Assume that $n > k \geq 3$ and that there exist some $a, b, u, v, c \in \mathbb{R}$ for which (1.4) holds. Consider derivatives of both sides of the identity. It is well known that the roots of $D_k(x,c)$ are all real when $c \geq 0$, see for instance [4, Sect. 6, p. 216], and so are also all the roots of the derivative $D_k'(x,c)$. Thus, if $c \geq 0$, then all the roots of $auD_k'(ux+v,c)$ are real, whereas $P_{n,k}'(x) = nP_{n-1,k-1}(x)$ has at most one real root by Lemma 2.4, a contradiction in view of $k-1 \geq 2$.

Therefore, in all what follows we will assume that $c < 0$ and $k \geq 4$. Suppose, by (1.4) and (3.2), that the identity

$$P_{n,k}(x) = aD_k(ux+v,c) + b = 2ac^{k/2}T_k((ux+v)/2\sqrt{c}) + b \tag{4.1}$$

holds. The roots of $T_k(x) = \cos(k \arccos x)$ are $x_j := \cos(\pi(2j-1)/2k)$, $j = 1, 2, \ldots, k$. Consequently, the roots of $T_k((ux+v)/2\sqrt{c})$ are $-v/u + 2\sqrt{c}x_j/u$, $j = 1, 2, \ldots, k$. They all lie on the vertical line $\Re(z) = -v/u$. Hence, by the Gauss-Lucas theorem, for $1 \leq j \leq k-1$, all the roots of $T_k^{(j)}((ux+v)/2\sqrt{c})$, where $T_k^{(j)}(x)$ denotes the jth derivative of $T_k(x)$, lie on the line $\Re(z) = -v/u$ as well. By taking $k-3$ derivatives of both sides of (4.1), we obtain

$$n(n-1)\ldots(n-k+4)P_{n-k+3,3}(x) = a2^{4-k}c^{3/2}u^{k-3}T_k^{(k-3)}((ux+v)/2\sqrt{c}).$$

By Lemma 2.4, the polynomial on the left hand side has exactly one real root. The roots of the polynomial on the right hand side are all on the line $\Re(z) = \omega := -v/u$, so the only real root is ω. Since the other two roots lying on $\Re(z) = \omega$ are also roots of the polynomial with real coefficients

$$P_{N,3}(x) = \binom{N}{3}x^3 + \binom{N}{2}x^2 + \binom{N}{1}x + 1,$$

where $N = n-k+3 \geq 4$, they must be of the form $\omega + i\tau$ and $\omega - i\tau$ for some $\tau > 0$. The sum of these three roots is

$$3\omega = \frac{-\binom{N}{2}}{\binom{N}{3}} = \frac{-3}{N-2},$$

wherefrom we get $\omega = -1/(N-2)$. Therefore, from

$$0 = P_{N,3}(\omega) = P_{N,3}\Big(-\frac{1}{N-2}\Big) = \frac{(N-3)(N-4)}{3(N-2)^2}$$

we derive that the only possibility is $N = 4$, i.e. $n = k + 1$.

It remains to investigate the case $n = k+1$ for $k \geq 4$. To that end rewrite (4.1) in the form

$$(1+x)^{k+1} - x^{k+1} = 2ac^{k/2}T_k((ux+v)/2\sqrt{c}) + b. \tag{4.2}$$

As the roots of the polynomial on the left hand side all lie on the line $\Re(z) = -1/2$, and those of the polynomial on the right hand side all lie on the line $\Re(z) = -v/u$, we must have $u = 2v$. Recall that $c < 0$. Writing $c = -1/w^2$ for some $w > 0$ we deduce that $(ux+v)/2\sqrt{c} = -ivw(x+1/2)$. Therefore, (4.2) can be rewritten as

$$(1+x)^{k+1} - x^{k+1} = 2aw^{-k}i^kT_k(-ivw(x+1/2)) + b. \tag{4.3}$$

From (3.2) it follows that $T_k(-ivwx) = 2^{k-1}(vw)^k(-i)^kD_k(x, -1/4v^2w^2)$. (This can be checked separately for $v > 0$ and $v < 0$. Note that clearly $v \neq 0$). By replacing x by $x - 1/2$ in (4.3) we obtain

$$\left(x+\frac{1}{2}\right)^k - \left(x-\frac{1}{2}\right)^k = a2^kv^kD_k(x, -1/4v^2w^2) + b. \tag{4.4}$$

Suppose that $k > 4$. Using the expansion (1.3) we find that the first three nonzero terms (with highest powers of x) on the right hand side of (4.4) are

$$a2^kv^kx^k + a2^kv^k\frac{k}{4v^2w^2}x^{k-2} + a2^kv^k\frac{k(k-3)}{32v^4w^4}x^{k-4} + \cdots.$$

The highest three nonzero terms on the left hand side of (4.4) are

$$\binom{k+1}{1}x^k + \binom{k+1}{3}x^{k-2}2^{-2} + \binom{k+1}{5}x^{k-4}2^{-4} + \cdots \tag{4.5}$$

By comparing the leading coefficients on both sides of (4.4) we get $a2^kv^k = k+1$. Comparison of the next two nonzero coefficients then yields

$$(k+1)k = v^2w^2\binom{k+1}{3}, \quad (k+1)k(k-3) = 2v^4w^4\binom{k+1}{5},$$

wherefrom $3(k-2) = 5(k-1)$, a contradiction.

Let now $k = 4$. Then $n = 5$. Since $D_4(x, c) = x^4 - 4cx^2 + 2c^2$, the equation (4.4) can be rewritten as

$$\left(x+\frac{1}{2}\right)^5 - \left(x-\frac{1}{2}\right)^5 = 16av^4\left(x^4 + \frac{1}{v^2w^2}x^2 + \frac{1}{8v^4w^4}\right) + b$$

Using (4.5) we get $a = 5/(16v^4)$, $v^2w^2 = 2$ and $b = -3/32$. Thus, $c = -v^2/2$. It is easy to check that with these values the identity $aD_4(ux+v, c) + b =$

$P_{5,4}(x)$ holds. Indeed,

$$\begin{aligned} aD_4(ux+v,c)+b &= \frac{5}{16v^4}D_4(v(2x+1),-v^2/2)-\frac{3}{32} \\ &= \frac{5}{16v^4}\left(v^4(2x+1)^4+4v^2(2x+1)^2\frac{v^2}{2}+\frac{v^4}{2}\right)-\frac{3}{32} \\ &= (1+x)^5-x^5=P_{5,4}(x). \end{aligned}$$

This completes the proof of the lemma. □

5. Proof of Theorem 1.2

We are now ready to prove one of our main results, namely, Theorem 1.2.

Proof of Theorem 1.2. For $m=3$ the theorem follows from Lemma 3.3. Assume henceforth $m\ge 4$. If the equation (1.2) has infinitely many integer solutions, then from Theorem 3.1 it follows that

$$(1+a_0+a_1x)^n-(a_0+a_1x)^n=\phi(f(x)), \tag{5.1}$$

$$(1+b_0+b_1x)^m-(b_0+b_1x)^m=\phi(g(x)), \tag{5.2}$$

where $(f(x),g(x))$ is a standard pair over $\mathbb{Q}$, $a_0,a_1,b_0,b_1\in\mathbb{Q}$, $a_1b_1\ne 0$ and $\phi(x)\in\mathbb{Q}[x]$. Assume that $h:=\deg\phi>1$. Then from Proposition 2.8 it follows that $1\le \deg f,\deg g\le 2$. Since $n>m$, we must have $\deg f=2$ and $\deg g=1$. In view of $\deg g=1$ there exist $g_0,g_1\in\mathbb{Q}$ such that $g_1\ne 0$ and $(1+g_0+g_1x)^m-(g_0+g_1x)^m=\phi(x)$, so that by (5.1) and (5.2),

$$\begin{aligned} (1+g_0+g_1f(x))^m-(g_0+g_1f(x))^m &= \phi(f(x)) \\ &= (1+a_0+a_1x)^n-(a_0+a_1x)^n. \end{aligned}$$

Since $\deg f=2$, by making the substitution $x\mapsto (x-a_0)/a_1$, we see that there exist $c_2,c_1,c_0\in\mathbb{Q}$, $c_2\ne 0$, such that

$$(1+c_2x^2+c_1x+c_0)^m-(c_2x^2+c_1x+c_0)^m=(1+x)^n-x^n.$$

Now, as $c_2\ne 0$, from Proposition 2.8 it follows that $c_2=c_1$ and that $(1+c_1x+c_0)^m-(c_1x+c_0)^m=\tilde{P}_{n,n-1}(x)$. However, all the roots of $\tilde{P}_{n,n-1}(x)$ are real, by (2.5), while $(1+c_1x+c_0)^m-(c_1x+c_0)^m=P_{m,m-1}(c_1x+c_0)$ has at most one real root by Lemma 2.4. This is a contradiction in view of $m-1\ge 2$.

If $\deg\phi = 1$, then we have

$$(1+x)^n - x^n = e_1 f(c_1 x + c_0) + e_0, \tag{5.3}$$

$$(1+x)^m - x^m = e_1 g(d_1 x + d_0) + e_0, \tag{5.4}$$

where $(f(x), g(x))$ is a standard pair over $\mathbb{Q}$, $c_1, c_0, d_1, d_0, e_1, e_0 \in \mathbb{Q}$, and $c_1 d_1 e_1 \neq 0$. Clearly, by (5.3) and (5.4), $\deg f = n-1$ and $\deg g = m-1$. Note that $(f(x), g(x))$ cannot be a standard pair over $\mathbb{Q}$ of the second kind, since $n > m \geq 4$ and hence $3 \leq \deg g < \deg f$. If $(f(x), g(x))$ is a standard pair over $\mathbb{Q}$ of the fifth kind, then $g(x) = 3x^4 - 4x^3$, and hence $m = 5$. (The case when $f(x) = 3x^4 - 4x^3$ is symmetric.) Then from (5.4) it follows that $P_{5,4}(x) = e_1(d_1 x + d_0)^3(3(d_1 x + d_0) - 4) + e_0$, which is impossible, by Lemma 3.4. If $(f(x), g(x))$ is a standard pair over $\mathbb{Q}$ of the first kind, then either $f(x) = x^{n-1}$ or $g(x) = x^{m-1}$, i.e. either $P_{n,n-1}(x) = e_1(c_1 x + c_0)^{n-1} + e_0$ or $P_{m,m-1}(x) = e_1(d_1 x + d_0)^{m-1} + e_0$, which is again in contradiction with Lemma 3.4, since $n - 1 > m - 1 \geq 3$. Finally, if $(f(x), g(x))$ is a standard pair over $\mathbb{Q}$ of the third or of the fourth kind, then

$$P_{n,n-1}(x) = e_1 D_{n-1}(c_1 x + c_0, \alpha) + e_0,$$
$$P_{m,m-1}(x) = e_1 D_{m-1}(d_1 x + d_0, \beta) + e_0,$$

for some $\alpha, \beta \in \mathbb{Q} \setminus \{0\}$. Since $n - 1 > m - 1 \geq 3$, Lemma 1.3 implies that $(n, m) = (5, 4)$ and $\alpha, \beta < 0$. Then, as $\gcd(4, 3) = 1$, the pair $(f(x), g(x))$ must a standard pair over $\mathbb{Q}$ of the third kind, with $\alpha = a^3$ and $\beta = a^4$ for some $a \in \mathbb{Q} \setminus \{0\}$, which contradicts $\beta < 0$. □

6. Proof of Theorem 1.1

Proposition 6.1. *Let $n, k, m, l \in \mathbb{N}$ be such that $3 \leq k \leq n-1, 3 \leq l \leq m-1$ and $k \neq l$. If $P_{n,k}(x)$ and $P_{m,l}(x)$ are indecomposable, then the equation (1.1) has at most finitely many integer solutions.*

Proof. Assume to the contrary that the equation (1.1) has infinitely many integer solutions. Then from Theorem 3.1 it follows that

$$P_{n,k}(x) = \phi\left(f\left(ux + v\right)\right), \quad P_{m,l}(x) = \phi\left(g\left(u'x + v'\right)\right), \tag{6.1}$$

where $\phi(x) \in \mathbb{Q}[x]$, $u, u', v, v' \in \mathbb{Q}$, $uu' \neq 0$ and $(f(x), g(x))$ is a standard pair over $\mathbb{Q}$. If both $f(x)$ and $g(x)$ are linear polynomials, then, by comparison of degrees in (6.1), we get $k = l$, contrary to the assumption. Thus, either $\deg f \geq 2$ or $\deg g \geq 2$. If $\deg\phi > 1$, then either $P_{n,k}(x)$ or $P_{m,l}(x)$ is decomposable, contrary to the assumption. Hence $\deg\phi = 1$ and not both

$f(x)$ and $g(x)$ are linear polynomials. Therefore, writing $\phi(x) = e_1x + e_0$ we have

$$P_{n,k}(x) = e_1 f(ux + v) + e_0, \quad P_{m,l}(x) = e_1 g(u'x + v') + e_0, \tag{6.2}$$

with $\deg f = k$ and $\deg g = l$.

Note that $(f(x), g(x))$ cannot be a standard pair of the second kind since $k, l \geq 3$. If $(f(x), g(x))$ is a standard pair of the fifth kind, then either $f(x)$ or $g(x)$ is equal to $3x^4 - 4x^3$. Without loss of generality assume that $f(x) = 3x^4 - 4x^3$. Then, by (6.2), we have $P_{n,4}(x) = e_1(3(ux+v)-4)(ux+v)^3 + e_0$, which is impossible by Lemma 3.4. If $(f(x), g(x))$ is a standard pair of the first kind, then either $f(x) = x^k$ or $g(x) = x^l$. Without loss of generality assume that $f(x) = x^k$. Then $P_{n,k}(x) = e_1(ux + v)^k + e_0$, contradicting Lemma 3.4 in view of $k \geq 3$. Let $(f(x), g(x))$ be a standard pair of the third kind or of the fourth kind. By Lemma 1.3, it follows that $k, l \leq 4$. Since $k, l \geq 3$ and $k \neq l$, by assuming without restriction of generality that $k > l$, we must only check the impossibility of the case $(k, l) = (4, 3)$. If $(k, l) = (4, 3)$, then the pair of Dickson polynomials $(f(x), g(x))$ must be of the third kind (since $\gcd(4, 3) = 1$). Hence $f(x) = D_4(x, c^3)$ and $g(x) = D_3(x, c^4)$ for some $c \in \mathbb{Q}\setminus\{0\}$. Then $P_{m,3}(x) = e_1 D_3(u'x+v', c^4)+e_0$, which contradicts Lemma 1.3 in view of $c^4 > 0$. □

Proof of Theorem 1.1. For $k, l \geq 3$ the theorem holds, by Proposition 6.1 and Lemma 2.5. It remains to examine the case when either $k = 2$ or $l = 2$. Recall the assumption $k \neq l$ and assume without loss of generality that $l = 2$ and $k \geq 3$. Then the equation (1.1) can be rewritten as

$$2m(m-1)P_{n,k}(x) - m^2 + 2m = (m(m-1)y + m)^2.$$

By Proposition 3.2, it suffices to show that the polynomial of the left hand side has at least three simple roots (here $m, k \geq 3$, $n \geq 4$). We will show that all k roots of the polynomial $aP_{n,k}(x) + b$, where $a \neq 0$ and b are rational numbers, are simple under assumption of irreducibility of $P_{n-1,k-1}(x)$.

Write $aP_{n,k}(x)+b$ in the form $cf_1(x)^{d_1} \dots f_t(x)^{d_t}$, where $f_1(x), \dots, f_t(x) \in \mathbb{Q}[x]$ are distinct irreducible polynomials with constant terms equal to 1, with $c \in \mathbb{Q} \setminus \{0\}$ and $d_1, \dots, d_t \in \mathbb{N}$. If $aP_{n,k}(x) + b$ has a double root s, then s is the root of its derivative. Hence, by (2.2), we obtain $P_{n-1,k-1}(s) = 0$. Since $P_{n-1,k-1}(x)$ is irreducible and has constant term equal to 1, it must be one of the polynomials $f_i(x)$, say $f_1(x)$. Furthermore, $d_1 \geq 2$, since the derivative of the product $cP_{n-1,k-1}(x)^{d_1} \dots f_t(x)^{d_t}$ vanishes at $x = s$. The

degree consideration now leads to

$$k = \deg(aP_{n,k}(x)+b) = \deg(cP_{n-1,k-1}(x)^{d_1} \dots f_t(x)^{d_t}) \geq d_1(k-1) \geq 2(k-1),$$

a contradiction. □

Note that for $k = l = 2$ the equation $P_{n,2}(x) = P_{m,2}(y)$ may have infinitely many solutions. Indeed, consider, for example, the equation

$$P_{4,2}(x) = \frac{(6x+2)^2+2}{6} = P_{3,2}(y) = \frac{(6y+3)^2+3}{12},$$

which can be rewritten as $(6y+3)^2 - 2(6x+2)^2 = 1$. This is a Pell-type equation with infinitely many solutions $x, y \in \mathbb{N}$.

Acknowledgements. The first name author was supported by the Research Council of Lithuania Grant MIP-068/2013/LSS-110000-740. The second named author was supported by the Austrian Science Fund (FWF) through projects W1230-N13, P24302 and F5510-N26. The latter project is a part of the Special Research Program Quasi-Monte Carlo Methods: Theory and Applications.

References

[1] A. Baker, *Bounds for the solutions of hyperelliptic equations*, Proc. Cambridge Philos. Soc. **65** (1969), 439–444.

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

[3] F. Beukers, T.N. Shorey and R. Tijdeman, *Irreducibility of polynomials and arithmetic progressions with equal products of terms*, Number Theory in Progress **1** (1999), Walter de Gruyter, Berlin, 11-26.

[4] Y. Bugeaud and F. Luca, *On Pillai's Diophantine equation*, New York J. Math. **12** (2006), 193–217 (electronic).

[5] A. Dubickas, *Roots of unity as quotients of two roots of a polynomial*, J. Aust. Math. Soc. **92** (2012), 137–144.

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

[7] R. Ferguson, *Irreducible polynomials with many roots of equal modulus*, Acta Arith. **78** (1997), 221–225.

[8] M. Filaseta, A. Kumchev and D.V. Pasechnik, *On the irreducibility of a truncated binomial expansion*, Rocky Mountain J. Math. **37** (2007), 455–464.

[9] M.D. Fried and R.E. MacRae, *On the invariance of chains of fields*, Illinois J. Math. **13** (1969), 165–171.

[10] S.K. Khanduja, R. Khassa, S. Laishram, *Some irreducibility results for truncated binomial expansions*, J. Number Theory **131** (2011), 300–308.

[11] D. Kreso and Cs. Rakaczki, *Diophantine equations with Euler Polynomials*, Acta Arith. **161** (2013), 267–281.

[12] H. Levi, *Composite polynomials with coefficients in an arbitrary field of characteristic zero*, Amer. J. Math. **64** (1942), 389–400.

[13] J.F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. **23** (1922), 51–66; errata ibid. **23** (1922), 431.

[14] I. Scherbak, *Intersections of Schubert varieties and highest weight vectors in tensor products sl_{N+1}-representations*, preprint at `arXivmath:0409329v3`, 2004.

[15] A. Schinzel, *Polynomials with special regard to reducibility*, Cambridge Univ. Press, Cambridge, 2000.

[16] A. Schinzel, *Around Pólya's theorem on the set of prime divisors of a linear recurrence*, Diophantine equations, Tata Inst. Fund. Res. Stud. Math., 20, Tata Inst. Fund. Res., Mumbai, 2008, 225–233.

[17] C.L. Siegel, *The integer solutions of the equation $y^2 = ax^n + bx^{n-1} + \cdots + k$*, J. London Math. Soc. **1** (1926), 66–68.

[18] T. Stoll, *Diophantine equations involving polynomial families*, PhD thesis, TU Graz (2003).

[19] K. Yokoyama, Z. Li and I. Nemes, *Finding roots of unity among quotients of the roots of an integral polynomial*, in: Proceedings of the 1995 International Symposium on Symbolic and Algebraic Computation, ISSAC'95, Montreal, 10–12 July 1995, (ed. A. H. M. Levelt), ACM Press, New York, 1995, 85–89.

[20] M.E. Zieve and P. Müller, *On Ritt's polynomial decomposition theorems*, preprint at `arXiv:0807.3578v1`, 2008.

Department of Mathematics and Informatics, Vilnius University, Naugarduko 24, LT-03225 Vilnius, Lithuania

E-mail address: `arturas.dubickas@mif.vu.lt`

Institut für Analysis und Computational Number Theory (Math A), Technische Universität Graz, Steyrergasse 30/II, 8010 Graz, Austria

E-mail address: `kreso@math.tugraz.at`