New York Journal of Mathematics

New York J. Math. **21** (2015) 987–1001.

On common values of lacunary polynomials at integer points

Dijana Kreso

Abstract. For fixed $\ell \geq 2$, fixed positive integers $m_1 > m_2$ with $\gcd(m_1, m_2) = 1$ and $n_1 > n_2 > \cdots > n_\ell$ with $\gcd(n_1, \ldots, n_\ell) = 1$, and fixed rationals $a_1, a_2, \ldots, a_{\ell+1}, b_1, b_2$ which are all nonzero except for possibly $a_{\ell+1}$, we show the finiteness of integral solutions x, y of the equation

$$a_1 x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = b_1 y^{m_1} + b_2 y^{m_2},$$

when $n_1 \geq 3$, $m_1 \geq 2\ell(\ell-1)$, and $(n_1, n_2) \neq (m_1, m_2)$. In relation to that, we show the finiteness of integral solutions of equations of type $f(x) = g(y)$, where $f, g \in \mathbb{Q}[x]$ are of distinct degrees ≥ 3, and are such that they have distinct critical points and distinct critical values.

Contents

1. Introduction

Loosely speaking, polynomials with few terms are called lacunary. We write $a_1 x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1}$ with $a_1 a_2 \ldots a_\ell \neq 0$ for a lacunary polynomial with ℓ nonconstant terms. When $\ell = 1$, we call such polynomials binomials, when $\ell = 2$ trinomials, etc. Many classical Diophantine equations can be seen as equations in lacunary polynomials. For example, a defining equation of an elliptic curve $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Q}$, $4a^3 + 27b^2 \neq 0$, can be seen as an equation in lacunary polynomials. In this note we show the following.

Received July 31, 2015. Revised September 7, 2015.

2010 *Mathematics Subject Classification.* 11D41, 12E05, 12F10.

Key words and phrases. Diophantine equation, lacunary polynomial, monodromy group, Morse polynomial, polynomial decomposition.

The author is thankful for the support of the Austrian Science Fund (FWF) via projects W1230-N13, FWF-P24302 and F5510.

ISSN 1076-9803/2015

Theorem 1.1. *The equation*

$$a_1x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = b_1y^{m_1} + b_2y^{m_2} \tag{1.2}$$

with $\ell \geq 2$, $m_i, n_j \in \mathbb{N}$, $a_i, b_j \in \mathbb{Q}$, *and*

$$m_1 > m_2,\ \gcd(m_1, m_2) = 1, \quad n_i > n_j \text{ if } i > j,\ \gcd(n_1, \ldots, n_\ell) = 1, \tag{1.3}$$

$$a_1a_2 \cdots a_\ell b_1 b_2 \neq 0, \tag{1.4}$$

$$\text{either } n_1 \neq m_1,\ \text{or } n_1 = m_1 \text{ but } n_2 \neq m_2, \tag{1.5}$$

and $n_1 \geq 3$, $m_1 \geq 2\ell(\ell-1)$, *has at most finitely many solutions in integers* x, y.

We remark that Theorem 1.1 is not effective, i.e., it does not give a bound for the size of the largest solution of Equation (1.2). Namely, the theorem relies (indirectly, see the begining of Section 4 for details) on Siegel's classical theorem on integral points on curves, and is thus ineffective.

From Theorem 1.1 it follows that the equation

$$a_1x^{n_1} + a_2x^{n_2} + a_3 = b_1y^{m_1} + b_2y^{m_2} \tag{1.6}$$

where (1.3), (1.4) and (1.5) (with $\ell = 2$) hold and $n_1 \geq 3, m_1 \geq 4$, has only finitely many integer solutions. This is the main result of [17]. From the theorem it further follows that the equation

$$a_1x^{n_1} + a_2x^{n_2} + a_3x^{n_3} + a_4 = b_1y^{m_1} + b_2y^{m_2} \tag{1.7}$$

where (1.3), (1.4) and (1.5) (with $\ell = 3$) hold, and $n_1 \geq 3, m_1 \geq 12$, has only finitely many integer solutions. Equations of type (1.6) and (1.7), which are only special cases of (1.2), have been studied in [6, 7, 10, 16, 17, 20], etc. For example, a classical problem involving trinomials is to determine when the product of two consecutive integers equals the product of three consecutive integers, i.e., to solve the equation $x^3 - x = y^2 - y$ in integers. Mordell [16] solved this problem. Similarly, to determine when the product of two is a product of four or five consecutive integers, one needs to solve equations of type (1.2) with $\ell = 4$ or $\ell = 3$ (so of type (1.7)).

To the proof of Theorem 1.1 we use a finiteness criterion from [3] and results on decomposable (representable as a functional composition of two polynomials of degree greater than 1) lacunary polynomials. Of importance to us is a result of Zannier [23] which states that, loosely speaking, *over a field of characteristic* 0, *a polynomial with few terms and large degree cannot have an inner noncyclic composition factor of small degree.* We remark that this result was used in an another paper of Zannier [24] in which he proved Schinzel's conjecture: over fields of characteristic 0, for a fixed nonconstant polynomial g, the number of terms of $g \circ h$ tends to infinity as the number of terms of h tends to infinity. See also [19, p. 187] for Schinzel's partial result in this direction.

Of importance to us is further a result of Fried and Schinzel [11] on indecomposability of trinomials $b_1x^{m_1} + b_2x^{m_2} + b_3$ with $b_1, b_2, b_3 \in \mathbb{Q}$, $b_1b_2 \neq$

$0, m_1 > m_2 \geq 1$, $\gcd(m_1, m_2) = 1$. We give an alternative proof of this result (over an arbitrary field of characteristic 0). When $m_2 \leq 2$, one easily sees that the trinomial on the right-hand side of (1.2), with $\gcd(m_1, m_2) = 1$ and $b_1 b_2 \neq 0$, is Morse in the sense of [21, p. 39]. A polynomial is Morse if it has distinct critical points and distinct critical values. We show that from the main result of [3] it follows that two rational Morse polynomials with distinct degrees, both of which are ≥ 3, cannot have infinitely many equal values at integers. This generalizes the result of Mignotte and Pethő [15] on the finiteness of integral solutions of the equation $x^p - x = y^q - x$ with $p > q \geq 2$. This further yields shorter proofs of the results in [2, 6, 9, 14, 22].

There may exist infinitely many integer solutions of (1.2) when $\ell = 2$, $n_1 = m_1$ and $n_2 = m_2$. This clearly happens when $a_1 = b_1, a_2 = b_2, a_3 = 0$. There may also exist infinitely many integer solutions of (1.2) when $\ell = 2$, $n_1 = m_1$ and $n_2 \neq m_2$, if $m_1, n_1 \leq 3$ (see below). These possibilities are eliminated by assumptions (1.5) and $n_1 \geq 3, m_1 \geq 2\ell(\ell-1)$ of Theorem 1.1. The assumption on m_1 comes from the application of already mentioned Zannier's result [23]. The assumption on coprimality of n_i's is also needed to apply this result. (See Theorem 3.6 for Zannier's theorem and p. 9 for its application.) When $\ell = 2$ and $m_1 < 2\ell(\ell-1) = 4$, Equation (1.2) may have infinitely many integer solutions (for suitable coefficients). Indeed, by [17, Thm. 1], when $\ell = 2$ and

$$m_1 = n_1 = 3, \quad n_2 = m_2 = 2,$$
$$a_1^2 b_2^3 + a_2^3 b_1^2 = 0,$$
$$27 a_1^2 a_3 + 4 a_2^3 = 0,$$

or

$$m_1 = n_1 = 3, \quad n_2 = 2, m_2 = 1,$$
$$27 a_1^4 b_2^3 + a_2^6 b_1 = 0,$$
$$3 a_2^3 a_3 b_1 + 3 a_1^2 b_2^3 + a_2^3 b_2^2 = 0,$$

then

$$a_1 x^{n_1} + a_2 x^{n_2} + a_3 = b_1(\zeta x + \mu)^{m_1} + b_2(\zeta x + \mu)^{m_2}, \tag{1.8}$$

where in the former case $\zeta = -a_1 b_2/(a_2 b_1)$, $\mu = -2b_2/(3b_1)$, and in the latter $\zeta = -a_2^2/(3a_1 b_2)$, $\mu = 3a_1^2 b_2^2/(a_2^3 b_1)$. Equation (1.8) clearly has infinitely many rational solutions when $a_3 = 0$, and thus it may have infinitely many integer solutions, depending on the coefficients a_1, a_2, b_1, b_2. Finally, the asummption on coprimality of m_i's is needed for the application of the above described result of Fried and Schinzel. When $\gcd(m_1, m_2) > 1$, the trinomial on the left-hand side of (1.2) is clearly decomposable. Schinzel [20] removed assumption (1.3) on trinomials in [17, Thm. 1]. This resulted in many more special cases of (1.2) with $\ell = 2$, $a_1 a_2 b_1 b_2 \neq 0$, $m_1, n_1 \geq 3$, when there are infinitely many integer solutions.

2. Critical points and indecomposability

Throughout this section K is an arbitrary field. A polynomial $f \in K[x]$ with $\deg f > 1$ is called *indecomposable* (over K) if it cannot be written as the composition $f(x) = g(h(x))$ with $g, h \in K[x]$ and $\deg g > 1$, $\deg h > 1$. Otherwise, it is said to be *decomposable*. Any representation of f as a functional composition of polynomials of degree greater than 1 is said to be a *decomposition* of f. Any polynomial f with $\deg f > 1$ can be written as a composition of indecomposable polynomials, but not necessarily in a unique way. Ritt [18] completely described the extent of nonuniqueness of factorization of polynomials with complex coefficients with respect to functional composition. Find more about this topic in [25].

Definition 2.1. Given $f \in K[X]$ with $f' \neq 0$ the *monodromy group* $\mathrm{Mon}(f)$ is the Galois group of $f(X) - t$ over the field $K(t)$, viewed as a group of permutations of the roots of $f(X) - t$.

By Gauss's lemma it follows that $f(X)-t$ from Definition 2.1 is irreducible over $K(t)$. Since $f' \neq 0$, $f(X)-t$ is also separable. Let x be a root of $f(X)-t$ in the splitting field over $K(t)$. Then $\mathrm{Mon}(f)$ is the Galois group of the Galois closure of $K(x)/K(f(x))$, viewed as a transitive permutation group on the conjugates of x over $K(f(x))$. The well known theorem of Lüroth (see [19, p. 13]) provides a dictionary between decompositions of $f \in K[x]$ and fields between $K(f(x))$ and $K(x)$, which then correspond to groups between the two associated Galois groups: $\mathrm{Mon}(f)$ and the stabilizer of x in $\mathrm{Mon}(f)$. In this way, the study of decompositions of a polynomial, reduces to the study of subgroups of its monodromy group. Then f is indecomposable if and only if $\mathrm{Mon}(f)$ is a primitive permutation group (since a transitive group is primitive if point stabilizers are maximal subgroups). For more details about the Galois-theoretic setup for addressing decomposition questions, see [25].

For $f \in K[x]$ with $\mathrm{char}(K) \nmid \deg f$ and $\gamma \in \overline{K}$ let $\delta(f, \gamma)$ denote the degree of the greatest common divisor of $f(x) - \gamma$ and $f'(x)$ in $\overline{K}[x]$.

Lemma 2.2. *If $f, g, h \in K[x]$ are such that $\mathrm{char}(K) \nmid \deg f$ and*

$$f(x) = g(h(x))$$

with $\deg g > 1$, then there exists $\gamma \in \overline{K}$ such that $\delta(f, \gamma) \geq \deg h$.

Proof. Let $\gamma_0 \in \overline{K}$ be a root of g' (which exists since by assumption $\mathrm{char}(K) \nmid \deg g$, and hence $\deg g' = \deg g - 1 \geq 1$) and let $\gamma = g(\gamma_0)$. Then every root of $h(x) - \gamma_0$ is a root of both $f(x) - \gamma$ and of $f'(x)$. □

We have the following two corollaries of Lemma 2.2.

Corollary 2.3. *If $f \in K[x]$ is such that $\mathrm{char}(K) \nmid \deg f$, $\deg f > 1$ and $\delta(f, \gamma) \leq 1$ for all $\gamma \in \overline{K}$, then f is indecomposable.*

Corollary 2.4. *If $f \in K[x]$ is such that $\mathrm{char}(K) \nmid \deg f$, $\deg f > 1$ and $\delta(f,\gamma) \le 2$ for all $\gamma \in \overline{K}$, then f is either indecomposable or $f(x) = g(h(x))$ where $\deg h = 2$ and g is indecomposable.*

Lemma 2.2, Corollary 2.3 and Corollary 2.4 were used in [2, 8, 9, 14, 22] as a method for finding possible decompositions of a polynomial. In all of these papers, the polynomial under consideration had simple critical points. This brings us to the following definition and theorem from [21, p. 39].

Definition 2.5. Let K be a field and $f \in K[x]$ of degree n. Then f is Morse if the following holds: the zeros $\beta_1, \beta_2, \ldots, \beta_{n-1}$ of the derivative f' are simple and $f(\beta_i) \ne f(\beta_j)$ for $i \ne j$.

Theorem 2.6. *Let K be a field and let $f \in K[x]$ of degree $n > 1$ be Morse, with $\mathrm{char}(K) \nmid n$. Then the Galois group of $f(x) - t$ over $K(t)$ is the symmetric group S_n.*

In other words, the monodromy group $\mathrm{Mon}(f)$ of a Morse polynomial with coefficients in a field K, such that $\mathrm{char}(K) \nmid \deg f$, is symmetric. Theorem 2.6 was first proved by Hilbert [12]. Find a proof in [21, p. 41]. The proof there involves inertia groups at ramification points. An elementary proof (when $\mathrm{char}(K) \ne 2$) may be obtained as follows: it is well known that if $e_1, e_2, \ldots, e_k$ are the multiplicities of the roots of $f(x) - x_0$, where $f \in K[x]$ with $\mathrm{char}(K) \nmid \deg f$, $x_0 \in \overline{K}$ and $\mathrm{char}(K) \nmid e_i$ for all i's, then $\mathrm{Mon}(f)$ contains an element having cycle lengths $e_1, e_2, \ldots, e_k$. Find an elementary proof of this fact in [19, p. 56]. Let x_0 be a root of f'. Since the critical points of f are simple, and have distinct critical values, it follows that all the roots of $f(x) - f(x_0)$, but x_0, are of multiplicity 1, and x_0 is of multiplicity 2. So, unless $\mathrm{char}(K) = 2$, $\mathrm{Mon}(f)$ contains an element having cycle lengths $1, 1, \ldots, 1, 2$, i.e., $\mathrm{Mon}(f)$ contains a transposition. From Corollary 2.3 it follows that $\mathrm{Mon}(f)$ is also primitive. Since $\mathrm{Mon}(f)$ is primitive and contains a transposition, it is symmetric (by classical Jordan's theorem).

3. On decomposable lacunary polynomials

From now on, K is a field with $\mathrm{char}(K) = 0$. Let $f \in K[x]$ with $l > 0$ nonconstant terms be decomposable and write without loss of generality

$$f(x) = g(h(x)) \text{ with } g, h \in K[x],\ \deg g \ge 2, \deg h \ge 2, \tag{3.1}$$

$$h(x) \text{ monic and } h(0) = 0. \tag{3.2}$$

We may indeed do so, because if $f = g \circ h$ with $g, h \in K[x] \setminus K$, then there exists a linear polynomial $\mu \in K[x]$ so that $\mu \circ h$ is monic and $\mu(h(0)) = 0$, and clearly $f = \left(g \circ \mu^{(-1)}\right) \circ (\mu \circ h)$.

We use Corollary 2.3 to give an alternative proof of the result of Fried and Schinzel [11] on indecomposability of polynomials of type $a_1 x^{n_1} + a_2 x^{n_2} + a_3$ with $n_1 > n_2 \ge 1$, $\gcd(n_1, n_2) = 1$ and $a_1 a_2 \ne 0$.

Theorem 3.3. *Let K be a field with* $\operatorname{char}(K) = 0$. *Then $a_1x^{n_1} + a_2x^{n_2} + a_3$, with $a_1, a_2, a_3 \in K$, $a_1a_2 \neq 0$, $n_1 > n_2 \geq 1$, $(n_1, n_2) = 1$, is indecomposable.*

Proof. It is equivalent to show that $f(x) := a_1x^{n_1} + a_2x^{n_2}$ is indecomposable. Since $f'(x) = n_1a_1x^{n_1-1} + n_2a_2x^{n_2-1}$, we have

$$xf'(x) = n_1f(x) - a_2(n_1 - n_2)x^{n_2}. \tag{3.4}$$

Let $f = g \circ h$ with $\deg g \geq 2$ and $\deg h \geq 2$, where h is monic and $h(0) = 0$, as in (3.1) and (3.2). Then $g(0) = 0$ as well. Let γ_0 be a root of g' (which exists since by assumption $\deg g' \geq 1$) and let $\gamma = g(\gamma_0)$. Then $h(x) - \gamma_0$ divides both $f(x) - \gamma$ and $f'(x)$, and $\delta(f, \gamma) \geq \deg h \geq 2$ (see Lemma 2.2). Assume that there exist distinct roots α and β of $h(x) - \gamma_0$. Then $f'(\alpha) = f'(\beta) = 0$ and $f(\alpha) = f(\beta) = \gamma$. Then from (3.4) it follows that $\alpha^{n_2} = \beta^{n_2}$, and from $f'(\alpha) = f'(\beta) = 0$ it follows that $\alpha^{n_1} = \beta^{n_1}$. Since $\gcd(n_1, n_2) = 1$ (and there exist positive integers a and b so that $an_1 - bn_2 = 1$), it follows that $\alpha = \beta$. Therefore, $h(x) - \gamma_0$ has no two distinct roots. Since its roots are roots of $f'(x) = n_1a_1x^{n_1-1} + a_2n_2x^{n_2-1}$, it follows that $h(x) - \gamma_0 = hx^k$ for some $h \in K$ and $2 \leq k \leq n_2 - 1$. Thus $0 = h(0) = \gamma_0$ and $0 = f(0) = \gamma$. Since $\gamma_0 = 0$ (unique ramification point) it follows that $g'(x) = \tilde{g}x^{m-1}$, where $m = \deg g$ and $\tilde{g} \in K$. Since $g(0) = 0$ it follows that $g(x) = gx^m$. Then $f(x) = gx^m \circ hx^k$, so $a_2 = 0$, a contradiction. □

Corollary 3.5. *Let K be a field with* $\operatorname{char}(K) = 0$, $\gcd(n_1, n_2) = 1$, $n_2 \leq 2 < n_1$, *and $a_1, a_2, a_3 \in K$ with $a_1a_2 \neq 0$. Then $a_1x^{n_1} + a_2x^{n_2} + a_3$ is Morse.*

Proof. It is equivalent to show that $f(x) := a_1x^{n_1} + a_2x^{n_2}$ is Morse. Clearly, f' has simple zeros, and f has distinct critical values since

$$xf'(x) = n_1f(x) - a_2(n_1 - n_2)x^{n_2}$$

and $(n_1, n_2) = 1$. See the proof of Theorem 3.3. □

The main ingredients of the proof of Theorem 1.1, besides the finiteness criterion of Bilu and Tichy [3], are Theorem 3.3, the well known Hajós lemma on the multiplicities of roots of lacunary polynomials (see Lemma 3.9 below) and the following result of Zannier [23] on decomposable lacunary polynomials.

Theorem 3.6. *Let K be a field with* $\operatorname{char}(K) = 0$, *and let $f \in K[x]$ have $\ell > 0$ nonconstant terms. Assume that $f = g \circ h$, where $g, h \in K[x]$ and where $h(x)$ is not of type $ax^k + b$ for $a, b \in K$. Then*

$$\deg f + 2\ell(\ell - 1) \leq 2\ell(\ell - 1) \deg h. \tag{3.7}$$

In particular, $\deg g \leq 2\ell(\ell - 1)$.

Remark 3.8. Theorem 3.6 is stated in [23] with $\deg f + l - 1 \leq 2\ell(\ell-1) \deg h$ instead of (3.7), but proved with (3.7) (due to weaker conclusion at the end of the proof). The bound on $\deg g$ is the same regardless.

If $f \in K[x]$ with ℓ nonconstant terms and $\mathrm{char}(K) = 0$ is decomposable, write it as in (3.1) and (3.2). Then Theorem 3.6 implies that

$$\deg f + 2\ell(\ell-1) \leq 2\ell(\ell-1)\deg h$$

unless $h(x) = x^k$. Note that

$$a_1 x^{n_1} + a_2 x^{n_2} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = f(x) = g(x) \circ x^k,$$

with distinct n_i's and $a_1 \cdots a_\ell \neq 0$, exactly when $k \mid n_i$ for all $i = 1, 2, \ldots, \ell$.

The main ingredients of the proof of Theorem 3.6 are the result of Brownawell and Masser [5] on vanishing sums in function fields, and the following result of Hajós, that will be of importance to us as well to the proof of Theorem 1.1.

Lemma 3.9 (Hajós's lemma)**.** *Let K be a field with $\mathrm{char}(K) = 0$. If $g \in K[x]$ with $\deg g \geq 1$ has a zero $\beta \neq 0$ of mutiplicity m, then g has at least $m+1$ terms.*

The proof of Lemma 3.9 can be found in [19, p. 187].

4. Diophantine equations with lacunary polynomials

To state the main result of [3], we need to define the so called "standard pairs" of polynomials. In what follows a and b are nonzero rational numbers, m and n are positive integers, r is a nonnegative integer, $p \in \mathbb{Q}[x]$ is a nonzero polynomial (which may be constant) and $D_m(x,a)$ is the m-th Dickson polynomial with parameter a given by

$$D_m(x,a) = \sum_{j=0}^{\lfloor m/2 \rfloor} \frac{m}{m-j} \binom{m-j}{j} (-1)^j a^j x^{m-2j}. \tag{4.1}$$

Standard pairs of polynomials over $\mathbb{Q}$ are listed in the following table.

kind	standard pair (or switched)	parameter restrictions
first	$(x^m, ax^r p(x)^m)$	$r < m, \gcd(r,m) = 1,\ r + \deg p > 0$
second	$(x^2, (ax^2+b)p(x)^2)$	-
third	$(D_m(x,a^n), D_n(x,a^m))$	$\gcd(m,n) = 1$
fourth	$(a^{\frac{-m}{2}} D_m(x,a), -b^{\frac{-n}{2}} D_n(x,b))$	$\gcd(m,n) = 2$
fifth	$((ax^2-1)^3, 3x^4 - 4x^3)$	-

Having defined the needed notions we now state the main result of [3].

Theorem 4.2. *Let $f, g \in \mathbb{Q}[x]$ be nonconstant polynomials. Then the following assertions are equivalent:*

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

$$f(x) = \phi\left(f_1\left(\lambda(x)\right)\right) \quad \& \quad g(x) = \phi\left(g_1\left(\mu(x)\right)\right), \tag{4.3}$$

where $\phi \in \mathbb{Q}[x]$, $\lambda, \mu \in \mathbb{Q}[x]$ are linear polynomials, and (f_1, g_1) 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.

Note that if the equation $f(x) = g(y)$ with nonconstant $f, g \in \mathbb{Q}[x]$ has only finitely many rational solutions with a bounded denominator, then it clearly has only finitely many integer solutions.

Find more abut the applications of Theorem 4.2 in [13].

The proof of Theorem 4.2 relies on Siegel's classical theorem on integral points on curves, and is consequently ineffective. For that reason, Theorem 1.1, as well as Theorem 4.5 below, are also ineffective.

Recall the Definition 2.5 of Morse polynomials.

Lemma 4.4. *Let $f \in \mathbb{C}[x]$ be Morse. If $f(x) = \alpha D_n(b_1 x + b_0, a) + \beta$ with $\alpha, \beta, a, b_1, b_0 \in \mathbb{C}$ and $a \neq 0$, where $D_n(x, a)$ is given by (4.1), then $n \leq 2$.*

Proof. Assume $n = \deg f \geq 3$. Since $\mathrm{Mon}(f)$ is symmetric by Theorem 2.6, it is in particular doubly transitive. This is the same as saying that

$$(f(x) - f(y))/(x - y)$$

is irreducible (see [19, p. 55]). This is not the case when f is of type $\alpha D_n(b_1 x + b_0, a) + \beta$, see [19, p. 52]. □

Theorem 4.5. *Let $f, g \in \mathbb{Q}[x]$ be Morse, and $\deg f \geq 3$, $\deg g \geq 3$ and $\deg f \neq \deg g$. Then the equation $f(x) = g(y)$ has at most finitely many integer solutions x, y.*

Proof. If the equation $f(x) = g(y)$ has infinitely many integer solutions, then

$$f(\lambda(x)) = \phi(f_1(x)), \quad g(\mu(x)) = \phi(g_1(x)), \tag{4.6}$$

where (f_1, g_1) is a standard pair over $\mathbb{Q}$, $\phi, \lambda, \phi \in \mathbb{Q}[x]$ and $\deg \lambda = \deg \mu = 1$.

Assume that $h := \deg \phi > 1$. Since f and g are Morse, it follows that they are indecomposable. Then $\deg f_1 = 1, \deg g_1 = 1$, and by (4.6) it follows that $f(x) = g(\ell(x))$ for some $\ell \in \mathbb{Q}[x]$, which contradicts $\deg f \neq \deg g$. If $\deg \phi = 1$, then we have

$$f(x) = e_1 f_1(c_1 x + c_0) + e_0, \quad g(x) = e_1 g_1(d_1 x + d_0) + e_0, \tag{4.7}$$

where $c_1, c_0, d_1, d_0, e_1, e_0 \in \mathbb{Q}$, and $c_1 d_1 e_1 \neq 0$. Let $\deg f = \deg f_1 =: k$ and $\deg g = \deg g_1 =: l$. By assumption $k, l \geq 3$.

Note that (f_1, g_1) cannot be a standard pair of the second kind, since $k, l > 2$. If (f_1, g_1) is a standard pair of the fifth kind, then either

$$f_1(x) = 3x^4 - 4x^3 \quad \text{and} \quad g_1(x) = (ax^2 - 1)^3,$$

or vice versa, but then by (4.7) both f' and g' have multiple roots, a contradiction with the assumption that f and g are Morse. If (f_1, g_1) is a standard pair of the first kind, then either $f_1(x) = x^k$ or $g_1(x) = x^l$, which is again

in contradiction with (4.7) and the fact that f' and g' have simple roots. Finally, if (f_1, g_1) is a standard pair of the third or of the fourth kind, then

$$f(x) = e_2 D_n(c_1 x + c_0, \alpha) + e_0, \quad g(x) = e_2 D_m(d_1 x + d_0, \beta) + e_0,$$

for some $e_2, \alpha, \beta \in \mathbb{Q} \setminus \{0\}$. However, by Lemma 4.4 this can not be. □

Corollary 4.8. *Let $a_1, a_2, a_3, b_1, b_2 \in \mathbb{Q}$ and $a_1 a_2 b_1 b_2 \neq 0$. Let further $n_1, n_2, m_1, m_2 \in \mathbb{N}$ be such that $n_2 < 3 \leq n_1$, $m_2 < 3 \leq m_1$, $\gcd(n_1, n_2) = 1$, $\gcd(m_1, m_2) = 1$ and $n_1 > m_1$. Then the equation*

$$a_1 x^{n_1} + a_2 x^{n_2} + a_3 = b_1 y^{m_1} + b_2 y^{m_2} \tag{4.9}$$

has only finitely many solutions in integers x, y.

Proof. It follows from Theorem 4.5 and Corollary 3.5. □

Corollary 4.8 generalizes the result of Mignotte and Pethő [15] on the finiteness of integral solutions of the equation $x^p - x = y^q - x$ with $p > q \geq 2$, except when $(p, q) = (3, 2)$. In this case we have

$$4x^3 - 4x + 1 = (2y - 1)^2,$$

and by the well known Baker's result [1], this equation has only finitely many solutions with an explicitly computable upper bound for the solutions. Confer [2, 6, 8, 9, 14, 22] where it is shown that certain families of polynomials are Morse (without mentioning that they are Morse or using Theorem 2.6). Theorem 4.5 above covers partially results in those papers (in most cases it is shown that for a certain familiy $(P_n)_n$ of polynomials for odd or for even n they are Morse, and for n of other parity, we have $\delta(f, \gamma) \leq 2$, as in Corollary 2.4). In our proof, we replaced comparison of coefficients in the study of standard pairs of third and fourth kind by Lemma 4.4.

Proving that the polynomial is Morse is not always simple. For instance, it is shown in [8] that the polynomial $P_{n,k}$, a truncation of the binomial expansion of $(1 + x)^n$ at the k-th step, is Morse for $k < n - 1$, provided no two roots, say ζ and ν, of $P_{n-1,k-1}$ are such that $\zeta^k = \nu^k$. For $n \leq 100$ and $k < n - 1$ no such two roots of $P_{n-1,k-1}$ exist. Proving this for any n and $k < n - 1$ seems not to be simple.

Proof of Theorem 1.1. If Equation (1.2) has infinitely many integer solutions, then

$$a_1 x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = \phi(f_1(\lambda(x))), \tag{4.10}$$

$$b_1 x^{m_1} + b_2 x^{m_2} = \phi(g_1(\mu(x))), \tag{4.11}$$

where (f_1, g_1) is a standard pair over $\mathbb{Q}$, $\phi, \lambda, \mu \in \mathbb{Q}[x]$ and $\deg \lambda = \deg \mu = 1$. Assume that $\deg \phi > 1$. Since $\gcd(m_1, m_2) = 1$, from Theorem 3.3 it follows that $\deg g_1 = 1$, so that $\phi(x) = b_1 \sigma(x)^{m_1} + b_2 \sigma(x)^{m_2}$ for some $\sigma \in \mathbb{Q}[x]$ with $\deg \sigma = 1$. Then

$$a_1 x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = (b_1 x^{m_1} + b_2 x^{m_2}) \circ \sigma(f_1(\lambda(x))). \tag{4.12}$$

From Theorem 3.6 it follows that either $\sigma(f_1(\lambda(x))) = \zeta x^k + \nu$ for some $\zeta, \nu \in \mathbb{Q}$ and $k = \deg f_1$, or $m_1 < 2\ell(\ell-1)$. The latter can not be by assumption. Note that if the former holds, then $k \mid n_i$ for all $i = 1, 2, \ldots, \ell$, which contradicts the assumption on coprimality of n_i's, unless $k = 1$. If $k = 1$, then $n_1 = m_1$. If $n_1 \neq m_1$, we are done. Assume henceforth $n_1 = m_1$ and

$$a_1 x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = b_1(\zeta x + \nu)^{n_1} + b_2(\zeta x + \nu)^{m_2} \tag{4.13}$$

If $\nu = 0$, then $\ell = 2$ and $m_2 = n_2$, a contradiction with the assumption (1.5). Assume henceforth $\nu \neq 0$. The polynomial on the right-hand side of (4.13) has a zero of multiplicity m_2, and the one on the left-hand side has no zero of multiplicity greater than ℓ (by Lemma 3.9), and thus $m_2 \leq \ell$. By assumption $n_1 = m_1 \geq 2\ell(\ell-1)$, so $m_1 - m_2 \geq \ell(2\ell-3) \geq \ell + 2$ when $\ell \geq 3$. If $\ell \geq 3$, then the polynomial on the right-hand side of (4.13) has more than $\ell + 1$ terms (since the coefficients of $x^{n_1}, x^{n_1-1}, \ldots, x^{m_2+1}$ are all nonzero), a contradiction. Thus $\ell = 2$ and hence

$$a_1 x^{n_1} + a_2 x^{n_2} + a_3 = b_1(\zeta x + \nu)^{n_1} + b_2(\zeta x + \nu)^{m_2}. \tag{4.14}$$

Then $m_2 \leq 2$ by Lemma 3.9. If $m_2 = 1$, then on the right-hand side we have a polynomial with nonzero coefficients to $x^{n_1}, x^{n_1-1}, \ldots, x^2$ (thus at least $n_1 - 1$ nonzero terms), and since $n_1 - 1 = m_1 - 1 \geq 3$ we have a contradiction, since on the left-hand side we have two nonconstant terms. If $m_2 = 2$, then by the same argument we must have $n_1 < 5$. By assumption we have $n_1 = m_1 \geq 4$, but $n_1 = 4$ can not be since then $\gcd(m_1, m_2) \neq 1$, a contradiction.

Thus $\deg \phi = 1$ and

$$a_1 x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} = e_1 f_1(c_1 x + c_0) + e_0, \tag{4.15}$$

$$b_1 x^{m_1} + b_2 x^{m_2} = e_1 g_1(d_1 x + d_0) + e_0, \tag{4.16}$$

where $c_1, c_0, d_1, d_0, e_1, e_0 \in \mathbb{Q}$, and $c_1 d_1 e_1 \neq 0$ and $\deg f = \deg f_1 = n_1$ and $\deg g = \deg g_1 = m_1$.

Note that (f_1, g_1) cannot be a standard pair of the second kind, since $n_1 > 2$ and $m_1 > 2$.

If (f_1, g_1) is a standard pair of the fifth kind, then either $g_1(x) = 3x^4 - 4x^3$ or $g_1(x) = (ax^2 - 1)^3$ for some $a \in \mathbb{Q}$. However, by Lemma 3.3,

$$b_1 x^{m_1} + b_2 x^{m_2} - e_0 = e_1 g_1(d_1 x + d_0)$$

has no roots of multiplicity greater than 2, a contradiction.

If (f_1, g_1) is a standard pair of the first kind, then either $g_1(x) = x^{m_1}$ or $f_1(x) = x^{n_1}$. Recall that $b_1 x^{m_1} + b_2 x^{m_2} - e_0$ has no root of multiplicity greater than 2. Since $m_1 \geq 4$, it can not be that $g_1(x) = x^{m_1}$. If $f_1(x) = x^{n_1}$, then $g_1(x) = cx^r p(x)^{n_1}$ where $c \in \mathbb{Q} \setminus \{0\}$, $r < n_1$, $\gcd(r, n_1) = 1$, $r + \deg p > 0$. If $\deg p > 0$, then since $n_1 \geq 3$ we have a contradiction, since $e_1 c(d_1 x + d_0)^r p(d_1 x + d_0)^{n_1} = b_1 x^{m_1} + b_2 x^{m_2} - e_0$, but $b_1 x^{m_1} + b_2 x^{m_2} - e_0$ has

no root of multiplicity greater than 2. Thus $\deg p = 0$ and $g_1(x) = c_1 x^{m_1}$ for some $c_1 \in \mathbb{Q} \setminus \{0\}$, which by the same argument can not be.

Finally, if (f_1, g_1) is a standard pair of the third or of the fourth kind, then $e_1 g_1(d_1 x + d_0) + e_0 = e_2 D_{m_1}(d_1 x + d_0, \beta) + e_0$ for some $e_2, \beta \in \mathbb{Q} \setminus \{0\}$, so that by (4.16), and by taking derivative, we get

$$b_1 m_1 x^{m_1 - 1} + b_2 m_2 x^{m_2 - 1} = e_2 d_1 D'_{m_1}(d_1 x + d_0, \beta).$$

We now show that $D'_{m_1}(x, \beta)$ has only simple roots, so that

$$e_2 d_1 D'_{m_1}(d_1 x + d_0, \beta)$$

has only simple roots as well. Recall $D_{m_1}(x, \beta) = 2\beta^{m_1/2} T_{m_1}(x/(2\sqrt{\beta}))$ where $T_k(x) = \cos(k \arccos x)$ is the kth Chebyshev polynomial of the first kind. Further recall that the roots of $T_k(x) = \cos(k \arccos x)$ are

$$x_j := \cos(\pi(2j - 1)/(2k)), \quad j = 1, 2, \ldots, k.$$

These are all simple and real, and thus all the roots of the derivative $D'_{m_1}(x, \beta) = \beta^{m_1/2 - 1} T'_{m_1}(x/(2\sqrt{\beta}))$ are simple as well (since the roots of $T'_{m_1}(x)$ are simple and real by Rolle's theorem). It follows that the roots of $b_1 m_1 x^{m_1 - 1} + b_2 m_2 x^{m_2 - 1}$ are simple, so that $m_2 \leq 2$. Finally

$$b_1 x^{m_1} + b_2 x^{m_2} - e_0 = e_2 D_{m_1}(d_1 x + d_0, \beta)$$

with $m_2 \leq 2$, can not be, by Corollary 3.5 and Lemma 4.4. □

Remark 4.17. In order to apply ideas used in the proof of Theorem 1.1 with the right-hand side of (1.2) replaced by a polynomial with a higher number of nonconstant terms, one would need an information about possible decompositions of this polynomial. No result of type (3.3) is known for lacunary polynomials with more than two nonconstant terms. One finds a partial result in this direction in [13] for the case of polynomials with three nonconstant terms. Furthermore, even if we had such information, technical details in the proof of Theorem 1.1 would be more challenging if on the right-hand side of (1.2) we a had polynomial with a higher number of nonconstant terms. Namely, the fact that a trinomial does not have a root of multiplicity greater than 2, (which follows from Lemma 3.9) is used repeatedly in the proof of Theorem 1.1. If the number of terms were greater, it would be harder to eliminate some standard pairs in the case $\deg \phi = 1$. For example, if (f_1, g_1) is a standard pair of the fifth kind, then either $g_1(x) = 3x^4 - 4x^3$ or $g_1(x) = (ax^2 - 1)^3$ for some $a \in \mathbb{Q}$, so it has a root of multiplicity 3. From (4.16) it follows that this cannot be, but we couldn't conclude that if on the left-hand side we had a polynomial with more than two nonconstant terms.

Remark 4.18. For a number field K, a finite set S of places of K containing all Archimedean places, and the ring of S-integers $\mathcal{O}_S$ of K, in [3, Thm. 10.5] it is classified when the equation $f(x) = g(y)$ with $f, g \in K[x]$ has infinitely many solutions with a bounded $\mathcal{O}_S$-denominator (i.e., infinitely many solutions $(x, y) \in K \times K$ for which there exists a nonzero $\delta \in \mathcal{O}_S$ such

that $\delta x, \delta y \in \mathcal{O}_S$). When K is totally real and S is the set of Archimedean places, then the same criterion as Theorem 4.2 (with "rational solutions with bounded denominator" replaced by "solutions with a bounded $\mathcal{O}_S$-denominator") holds. Note that all the results on decomposability of polynomials in (1.2) from Section 3 hold for polynomials over arbitrary field of characteristic 0. One easily sees that our proof of Theorem 1.1 extends to the case when the polynomials in (1.2) are over arbitrary totally real number field K, so that Equation (1.2) with assumptions of Theorem 1.1 has only finitely many solutions with a bounded $\mathcal{O}_S$-denominator. The only part of the proof that does not extend at once is in the last paragraph, where the possibility $\deg \phi = 1$ and (f_1, g_1) is a standard pair of the third or of the fourth kind is eliminated via Rolle's theorem. The use of Rolle's theorem can be replaced by comparison of coefficients in $b_1 x^{m_1} + b_2 x^{m_2} = e_2 D_{m_1}(d_1 x + d_0, \beta) + e_0$, as was done in [17, Lemma 5]. For simplicity, we have restricted our attention to the most prominent case, $K = \mathbb{Q}$ and $\mathcal{O}_S = \mathbb{Z}$.

As explained on p. 8, Theorem 1.1 is ineffective. In [17], where the case $\ell = 2$ of Theorem 1.1 is studied, an effective finiteness statement is given for the case when one of the trinomials in (1.2) is quadratic. In that case one may use a well-known effective result of Baker [1] on hyperelliptic equations. In [17], the authors used Brindza's [4] more general result, which states that for the equation $f(x) = y^2$, with $f \in \mathbb{Q}[x]$ with at least three zeros of odd multiplicity, there exists a constant c_1, depending only on f, such that for all solutions $(x, y) \in \mathbb{Z}^2$ of the equation, one has $\max(|x|, |y|) \leq c_1$. When $\ell = 2$ and $(n_1, n_2) = (2, 1)$ or $(m_1, m_2) = (2, 1)$, an effective finiteness result for Equation (1.2) (without assuming coprimality on m_i's or n_i's as in (1.3)) is given by [17, Thm. 2]. For $\ell \geq 2$ and $(m_1, m_2) = (2, 1)$, Equation (1.2) can be written as

$$4b_1 a_1 x^{n_1} + \cdots + 4b_1 a_\ell x^{n_\ell} + 4b_1 a_{\ell+1} + b_2^2 = (2b_1 y + b_2)^2. \tag{4.19}$$

If the polynomial on the left-hand side of (4.19) has at least three zeros of odd multiplicity, this equation has finitely many effectively computable integer solutions x, y. It is shown in [17] that, when $\ell = 2$, this holds when $4b_1 a_3 + b_2^2 \neq 0$ and, $n_1 \neq 2n_2$ or

$$(n_1, n_2) \notin \{(3, 1), (3, 2), (4, 1), (4, 3), (6, 2), (6, 4)\},$$

and when $4b_1 a_3 + b_2^2 = 0$ and either $n_1 - n_2 \geq 3$, or $n_1 - n_2 = 2$ and n_2 is odd. One can investigate other special cases of (1.2) with $(m_1, m_2) = (2, 1)$ and "small" $\ell \geq 3$ in a similar fashion. As that is not in the focus of the present paper, we don't present such investigations.

Another way to obtain effective results for Equation (1.2) is to use known effective results about superelliptic equations, which corresponds to the case when either $m_2 = 0$ or $\ell = 1$. If $m_2 = 0$, then

$$a_1 x^{n_1} + \cdots + a_\ell x^{n_\ell} + a_{\ell+1} - b_2 = b_1 y^{m_1} \tag{4.20}$$

and if $\ell = 1$, then

$$b_1 y^{m_1} + b_2 y^{m_2} - a_2 = a_1 x^{n_1}. \tag{4.21}$$

By Baker's result [1], Equations (4.20) and (4.21) with $m_1, n_1 \geq 3$, have finitely many effectively computable solutions x, y in integers, whenever the polynomials on the left-hand side have at least two simple zeros. For Equation (4.21) we may give more precise information. To that end we follow the approach from [17, Thm. 2].

By Lemma 3.9 the polynomial on the left-hand side of (4.21) has no zeros of multiplicity greater than 2. If it has no two simple zeros, then it is of type $b_1 y^{m_1} + b_2 y^{m_2} - a_2 = f(y)^2 \mu(y)$, where $f \in \mathbb{Q}[y]$ with $\deg f \geq 1$ has simple roots, and $\mu \in \mathbb{Q}[y]$ is of degree at most 1. Assume first $a_2 \neq 0$. Note that for any root ζ of f we have

$$\zeta^{m_1} = \frac{-a_2 m_2}{(m_1 - m_2) b_1}, \ \zeta^{m_2} = \frac{a_2 m_1}{(m_1 - m_2) b_2}. \tag{4.22}$$

If $d = \gcd(m_1, m_2)$ then from (4.22) it follows that for every root ζ of f the value ζ^d is the same. So, the number of roots of f, i.e., $\deg f$, is bounded by d. Since $\deg f \geq (m_1 - 1)/2$, it follows that $m_1 \leq 2 \gcd(m_1, m_2) + 1$, wherefrom either $m_1 = 2m_2$ or $(m_1, m_2) \in \{(3, 1), (3, 2)\}$. Thus, apart from these cases, Equation (4.21) with $m_1, m_2, n_1 \in \mathbb{N}$, $m_1, n_1 \geq 3$ and nonzero $b_1, b_2, a_1, a_2 \in \mathbb{Q}$, has only finitely many effectively computable solutions. If $a_2 = 0$, on the left-hand side of (4.21) we have $y^{m_2}(b_1 y^{m_1 - m_2} + b_2)$, which has at least two simple zeros exactly when $m_1 - m_2 \geq 2$.

References

[1] Baker, A. Bounds for the solutions of the hyperelliptic equation. *Proc. Cambridge Philos. Soc.* **65** (1969), 439–444. MR0234912 (38 #3226), Zbl 0174.33803, doi: 10.1017/S0305004100044418.

[2] Beukers, F.; Shorey, T. N.; Tijdeman, R. Irreducibility of polynomials and arithmetic progressions with equal products of terms. *Number Theory in Progress, Vol 1* (Zakopane-Kościelisko, 1997), 11–26. *de Gruyter, Berlin*, 1999. MR1689495 (2000c:11046), Zbl 0933.11011, doi: 10.1515/9783110285581.11.

[3] Bilu, Yuri F.; Tichy, Robert F. The Diophantine equation $f(x) = g(y)$. *Acta Arith.* **95** (2000), no. 3, 261–288. MR1793164 (2001i:11031), Zbl 0958.11049.

[4] Brindza, B. On S-integral solutions of the equation $y^m = f(x)$. *Acta Math. Hungar.* **44** (1984), no. 1–2, 133–139. MR0759041 (85m:11017), Zbl 0552.10009, doi: 10.1007/BF01974110.

[5] Brownawell, W. D.; Masser, D. W. Vanishing sums in function fields. *Math. Proc. Cambridge Philos. Soc.* **100** (1986), no. 3, 427–434. MR0857720 (87k:11080), Zbl 0612.10010, doi: 10.1017/S0305004100066184.

[6] Bugeaud, Yann; Luca, Florian. On Pillai's Diophantine equation. *New York J. Math.* **12** (2006), 193–217 (electronic). MR2242533 (2007d:11033), Zbl 1136.11026.

[7] Bugeaud, Yann; Mignotte, Maurice; Siksek, Samir; Stoll, Michael; Tengely, Szabolcs. Integral points on hyperelliptic curves. *Algebra Number Theory* **2** (2008), no. 8, 859–885. MR2457355 (2010b:11066), Zbl 1168.11026, arXiv:0801.4459, doi: 10.2140/ant.2008.2.859.

[8] Dubickas, Arturas; Kreso, Dijana. Diophantine equations with truncated binomial expansions. Preprint, to appear in *Indagationes Mathematicae*, 2015.

[9] Dujella, Andrej; Tichy, Robert F. Diophantine equations for second-order recursive sequences of polynomials. *Q. J. Math.* **52** (2001), no. 2, 161–169. MR1838360 (2002d:11030), Zbl 0997.11026, doi: 10.1093/qjmath/52.2.161.

[10] Fielder, Daniel C.; Alford, Cecil O. Observations from computer experiments on an integer equation. *Applications of Fibonacci numbers, Vol. 7* (Graz, 1996), 93–103. *Kluwer Acad. Publ., Dordrecht*, 1998. MR1638435, Zbl 0913.11014, doi: 10.1007/978-94-011-5020-0_13.

[11] Fried, M.; Schinzel, A. Reducibility of quadrinomials. *Acta Arith.* **21** (1972), 153–171. MR0313219 (47 #1774), Zbl 0216.04601.

[12] Hilbert, David. Ueber die Irreducibilität ganzer rationaler Functionen mit ganzzahligen Coefficienten. *J. Reine Angew. Math.* **110** (1892), 104–129. MR1580277, JFM 24.0398.05.

[13] Kreso, Dijana; Tichy, Robert F. Functional composition of polynomials: indecomposability, Diophantine equations and lacunary polynomials. arXiv:1503.05401.

[14] Kulkarni, Manisha; Sury, B. On the Diophantine equation $1+x+\frac{x^2}{2!}+\cdots+\frac{x^n}{n!}=g(y)$. Diophantine equations, 121–134, Tata Inst. Fund. Res. Stud. Math., 20. *Tata Inst. Fund. Res., Mumbai*, 2008. MR1500222 (2010h:11046), Zbl 1194.11041.

[15] Mignotte, M.; Pethő, A. On the Diophantine equation $x^p - x = y^q - y$. *Publ. Mat.* **43** (1999), no. 1, 207–216. MR1697521 (2000d:11044), Zbl 0949.11022, doi: 10.5565/PUBLMAT_43199_08.

[16] Mordell, L. J. On the integer solutions of $y(y+1) = x(x+1)(x+2)$. *Pacific J. Math.* **13** (1963), 1347–1351. MR0153627 (27 #3590), Zbl 0124.27402, doi: 10.2140/pjm.1963.13.1347.

[17] Péter, Gyöngyvér; Pintér, Ákos; Schinzel, Andrzej. On equal values of trinomials. *Monatsh. Math.* **162** (2011), no. 3, 313–320. MR2775849 (2012b:11052), Zbl 1296.11021, doi: 10.1007/s00605-009-0169-0.

[18] Ritt, J. F. Prime and composite polynomials. *Trans. Amer. Math. Soc.* **23** (1922), no. 1, 51–66. MR1501189, JFM 48.0079.01, doi: 10.2307/1988911.

[19] Schinzel, A. Polynomials with special regard to reducibility. Encyclopedia of Mathematics and its Applications, 77. *Cambridge University Press, Cambridge*, 2000. x+558 pp. ISBN: 0-521-66225-7. MR1770638 (2001h:11135), Zbl 0956.12001.

[20] Schinzel, A. Equal values of trinomials revisited. *Tr. Mat. Inst. Steklova* **276** (2012), Teoriya Chisel, Algebra i Analiz, 255–261; translation in *Proc. Steklov Inst. Math.* **276** (2012), no. 1, 250–256. ISBN: 5-7846-0121-0; 978-5-7846-0121-6. MR2986125, Zbl 06345319, doi: 10.1134/S008154381201021X.

[21] Serre, Jean-Pierre. Topics in Galois theory. Lecture notes prepared by Henri Darmon. Research Notes in Mathematics, 1. *Jones and Bartlett Publishers, Boston, MA*, 1992. xvi+117 pp. ISBN: 0-86720-210-6. MR1162313 (94d:12006), Zbl 0746.12001.

[22] Stoll, Thomas. Diophantine equations involving polynomial families. Ph.D. Thesis, TU Graz, 2003.

[23] Zannier, Umberto. On the number of terms of a composite polynomial. *Acta Arith.* **127** (2007), no. 2, 157–167. MR2289981 (2008a:12003), Zbl 1161.11003, doi: 10.4064/aa127-2-5.

[24] Zannier, Umberto. On composite lacunary polynomials and the proof of a conjecture of Schinzel. *Invent. Math.* **174** (2008), no. 1, 127–138. MR2430978 (2009f:11032), Zbl 1177.12004, arXiv:0705.0911, doi: 10.1007/s00222-008-0136-8.

[25] Zieve, Michael E.; Müller, Peter. On Ritt's polynomial decomposition theorems. Preprint, 2008. arXiv:0807.3578.

(Dijana Kreso) Institut für Analysis und Computational Number Theory (Math A), Technische Universität Graz, Steyrergasse 30/II, 8010 Graz, Austria
kreso@math.tugraz.at

This paper is available via http://nyjm.albany.edu/j/2015/21-45.html.