POLYNOMIALS DETERMINED BY A FEW OF THEIR COEFFICIENTS

K. Győry[1,2], L. Hajdu[1,3], Á. Pintér[1,3,4] and A. Schinzel

We prove some results which indicate that a monic polynomial over a field of characteristic zero with exactly k distinct zeros may be determined up to finitely many possibilities by any k of its non-zero proper coefficients.

1. Introduction

There are only few results in the literature about the number (multiplicities) of the zeros of the sum of two polynomials where one of them is fixed; see e.g. [7], [4], [2], and the references given there. A related problem is the following: when is it true that a polynomial is "determined" by a "few" of its coefficients? In the present paper we obtain some results in this direction. Further, we give an application to superelliptic equations.

2. Results

Throughout the paper, K will denote an arbitrary field of characteristic zero. First we formulate the following

Problem. *Is it true that a monic polynomial $f \in K[x]$ of degree n with exactly k distinct zeros is determined up to finitely many possibilities by any k of its non-zero proper coefficients?*

We consequently write $f(x) = x^n + \sum_{i=1}^{n} a_i x^{n-i}$ with $a_i \in K$ and call a_i the proper coefficients of f. When we say that a_i $(i \in I)$ are given, we mean that we have the values (i, a_i) for $i \in I$.

An affirmative answer to the above Problem is supported by the next four theorems. By $[y]$ we will denote the integer part of $y \in \mathbb{R}$.

2000 Mathematics Subject Classification: 11C08, 11D41.
[1]Research supported in part by the Hungarian Academy of Sciences, the Netherlands Organization for Scientific Research (NWO) and by grant T042985 of the Hungarian National Foundation for Scientific Research (HNFSR).
[2]Research supported in part by grant T038225 of the HNFSR.
[3]Research supported in part by grant F034981 of the HNFSR and by the FKFP grant 3272-13/066/2001.
[4]Research supported in part by the János Bolyai Research Fellowship.

Theorem 1. *If a monic polynomial $f \in K[x]$ of degree n has exactly two distinct zeros, then it is determined up to $n(n-1)\left[\frac{n}{2}\right]$ possibilities by any two of its non-zero proper coefficients.*

Remark 1. The examples $f(x) = x^3 + ax^2$ and $x^4 + 2ax^2 + a^2$ show that there exist infinitely many polynomials of the same degree with exactly two distinct zeros and two coefficients equal to 0.

Theorem 2. *If a monic polynomial $f \in K[x]$ of degree n has a zero of multiplicity at least m, then it is determined up to n possibilities by any $n-m+1$ of its non-zero proper coefficients.*

In the special case when the first few coefficients are fixed we prove

Theorem 3. *Let $n_1, \dots, n_k$ be positive integers with $n_1+\dots+n_k = n$ and $a_1, \dots, a_k$ given elements of K. Then there exist at most $k!$ polynomials*

$$f(x) = x^n + a_1x^{n-1} + \dots + a_kx^{n-k} + g(x), \quad \deg g < n-k \tag{1}$$

in $K[x]$ such that $f(x)$ has exactly k distinct zeros with multiplicities $n_1, \dots, n_k$, respectively.

Remark 2. It follows that there are $k!p(n,k)$ polynomials f in $K[x]$ with $a_1, \dots, a_k$ given and exactly k distinct zeros, where $p(n,k)$ is the number of partitions of n into k positive integer summands.

The following result shows that for polynomials of degree at most six, the answer to our Problem is affirmative.

Theorem 4. *Let $f \in K[x]$ be a monic polynomial of degree n with $n \le 6$, having exactly k distinct zeros $(1 \le k \le n)$. Then f is determined up to c possibilities by any k of its non-zero proper coefficients. Here c denotes an absolute constant, which can be given explicitly.*

Theoretically, for each value of n one can find the answer to the problem, but the required amount of computation increases quickly with n.

The following related theorems are motivated by their applications to superelliptic diophantine equations. From now on till the end of this section we assume $K = \mathbb{Q}$.

Theorem 5. *Let l be an integer with $l \ge 2$. If f has at most one zero of multiplicity not divisible by l, then f is determined by the coefficients $a_1, \dots, a_{m+1}$, where $m = [(n-1)/l]$. More precisely, in this case $(a_{m+2}, \dots, a_{n-1}, a_n)$ can attain at most $m+1$ different tuples, which can be effectively determined in terms of $a_1, \dots, a_{m+1}, m, l$.*

We now show that the bounds given in Theorem 5 are sharp.

Proposition. *Keeping the notation of Theorem 5, the following statements hold.*

i) For any $a_1, \dots, a_m$ there are infinitely many $(a_{m+1}, \dots, a_n)$ such that f has at most one zero of multiplicity not divisible by l.

ii) For any l there exist infinitely many tuples $(a_1, \dots, a_{m+1})$ admitting exactly $m+1$ tuples $(a_{m+2}, \dots, a_n)$ such that f has at most one zero of multiplicity not divisible by l.

Theorem 6. *If f has at most two zeros of odd multiplicities, then f is determined by the coefficients $a_1, \dots, a_{m+2}$, where $m = [(n-2)/2]$. More precisely, in this case $(a_{m+3}, \dots, a_{n-1}, a_n)$ can attain at most $[(m+2)/2](m+1)(m+2)/2$ different tuples, and these tuples can be effectively determined in terms of $a_1, \dots, a_{m+2}, m$.*

On combining our Theorems 5 and 6 with a result of Brindza [1] we get the following consequence concerning superelliptic equations.

Corollary. *Let $f(x) \in \mathbb{Q}[x]$ be as above. Further, let l be an integer with $l \geq 2$ and $\varepsilon = 2$ if $l = 2$ and 1 if $l > 2$. Put $m = [(n-\varepsilon)/l]$ and*

$$N = \begin{cases} m+1, & \text{if } l > 2, \\ [(m+2)/2](m+1)(m+2)/2, & \text{if } l = 2. \end{cases}$$

Apart from at most N polynomials $g(x) \in \mathbb{Q}[x]$ of degrees less than $n - m - \varepsilon$, the equation

$$f(x) + g(x) = by^l \quad \text{for given } b \in \mathbb{Q} \setminus \{0\} \text{ and for each given } g,$$

has only finitely many solutions $x, y \in \mathbb{Z}$, and these solutions can be effectively determined. Moreover, the exceptional polynomials $g(x)$ can also be effectively determined.

The first result of this type was obtained in [7]. For further related results, we refer to [2].

We note that Theorem 3 has a similar consequence for superelliptic equations.

3. Proofs

In the proofs of Theorems 1 to 4, we deal with polynomials with coefficients from a field K of characteristic 0. To prove Theorem 1, we need the following lemma.

Lemma 1. *If the polynomials $f, g \in K[x, y]$ are homogeneous of degrees i and j, respectively, and the elements a, b of K are not both 0, then the system of equations*

$$f(x, y) = a, \quad g(x, y) = b \tag{2}$$

has at most ij solutions in the algebraic closure of K, unless there exists an $h \in K[x, y]$ such that

$$f(x, y) = ah(x, y)^{i/(i,j)}, \quad g(x, y) = bh(x, y)^{j/(i,j)}.$$

Proof. By Bézout's theorem, if the system (2) has more than ij solutions, then

$$(f(x, y) - a, g(x, y) - b) \neq 1.$$

Putting $x = ty$ we infer that

$$(y^i f(t, 1) - a, y^j g(t, 1) - b) \neq 1.$$

Moreover, the greatest common divisor of two binomials of degrees i, j over a field L, is either a binomial of degree (i, j), or an element of L (see [6]). Hence, taking $L = K(t)$, we infer the existence of a polynomial $h \in K(t)$ such that

$$(y^{(i,j)} h(t) - 1) \mid (y^i f(t) - a), \quad (y^{(i,j)} h(t) - 1) \mid (y^j g(t) - b),$$

hence

$$f(t) = ah(t)^{i/(i,j)}, \quad g(t) = bh(t)^{j/(i,j)}.$$

□

Proof of Theorem 1. Assume that f has the zeros ξ_i with multiplicity n_i $(i = 1, 2)$, $n_1 + n_2 = n$. Then we have

$$(-1)^i a_i = \tau_i(\underbrace{\xi_1, \dots, \xi_1}_{n_1}, \underbrace{\xi_2, \dots, \xi_2}_{n_2}) \quad (i = 1, \dots, n),$$

where τ_i is the i-th fundamental symmetric function. Put

$$f_i(x_1, x_2) = \sum_{i_1+i_2=i} \binom{n_1}{i_1}\binom{n_2}{i_2} x_1^{i_1} x_2^{i_2} \quad (i = 1, \dots, n).$$

Clearly,

$$\tau_i(\underbrace{\xi_1, \dots, \xi_1}_{n_1}, \underbrace{\xi_2, \dots, \xi_2}_{n_2}) = f_i(\xi_1, \xi_2) \quad (i = 1, \dots, n).$$

Since the number of decompositions $n = n_1 + n_2$, where $1 \le n_1 \le n_2$ is $\left[\frac{n}{2}\right]$, it suffices, by virtue of Lemma 1, to prove that for $i, j \in \{1, \dots, n\}$, $i \ne j$ there exists no polynomial $h \in K[x, y]$ such that

(3) $$f_i(x, y) = a_i h(x, y)^{i/d}, \quad f_j(x, y) = a_j h(x, y)^{j/d}, \quad d = (i, j)$$

(the factors $(-1)^i$ and $(-1)^j$ have been incorporated into $h(x, y)^{i/d}$ and and $h(x, y)^{j/d}$, respectively). Without loss of generality we may assume that $i < j$ and $n_1 \le n_2$. We shall consider successively the following cases

(4) $$j \le n_1,$$

(5) $$i \le n_1 < j,$$

(6) $$n_1 < i.$$

In the case (4) let $h(x, y) = \sum_{\delta=0}^{d} b_\delta x^{d-\delta} y^\delta$. We obtain from equations (3) that

$$\binom{n_1}{i} = a_i b_0^{i/d}, \quad \binom{n_1}{i-1} n_2 = a_i \frac{i}{d} b_0^{i/d-1} b_1.$$

Hence $b_0 \ne 0$ and on dividing side by side we get

$$\frac{i n_2}{n_1 - i + 1} = \frac{i b_1}{d b_0}.$$

It follows that $b_1 \ne 0$ and $n_1 - i + 1 = d n_2 b_0 / b_1$. Similarly, $n_1 - j + 1 = d n_2 b_0 / b_1$. Hence $i = j$, a contradiction.

In the case (5) we have $f_i(x,y) \not\equiv 0 \pmod{y}$, $f_j(x,y) \equiv 0 \pmod{y}$, hence (3) is impossible.

In the case (6) $f_i(x,y)$ is divisible exactly by y^{i-n_1}, $f_j(x,y)$ is divisible exactly by y^{j-n_1}. So if $h(x,y)$ is divisible exactly by y^k, we obtain

$$i - n_1 = ki/d, \quad j - n_1 = kj/d,$$

and consequently,

$$i\left(1 - \frac{k}{d}\right) = n_1 = j\left(1 - \frac{k}{d}\right).$$

Since $n_1 \neq 0$, we get $i = j$, a contradiction.

Thus (3) cannot hold in any of the cases (4-6), and the theorem follows. □

To prove Theorem 2, we need a lemma.

Lemma 2. *Let $x_1, \dots, x_d$ be unknowns, and write $\binom{x_i}{u} = \prod_{j=0}^{u-1} (x_i - j)/u!$ for $i = 1, \dots, d$ and for any non-negative integer u. Then we have*

$$\begin{vmatrix} 1 & \cdots & 1 \\ \binom{x_1}{1} & \cdots & \binom{x_d}{1} \\ \vdots & \vdots & \vdots \\ \binom{x_1}{d-1} & \cdots & \binom{x_d}{d-1} \end{vmatrix} = \frac{\prod_{1 \le i < j \le d} (x_j - x_i)}{0!1!\dots(d-1)!}.$$

Proof. By a suitable multiplication and addition of rows the determinant reduces to the Vandermonde determinant. □

Proof of Theorem 2. Let ξ be a zero of f of order at least m. If $\xi = 0$, then the last m coefficients of f are 0, hence there are at most $n - m$ non-zero proper coefficients of f and the assertion of the theorem is void. Hence assume that $\xi \neq 0$. We have

$$(7) \qquad \frac{1}{j!} f^{(j)}(\xi) = \binom{n}{j} \xi^{n-j} + \sum_{i=1}^{n} a_i \binom{n-i}{j} \xi^{n-i-j} = 0 \quad (0 \le j < m).$$

Assume that the a_i are given for $i \in I = \{i_m, i_{m+1}, \dots, i_n\}$ and that

$$\{1, \dots, n\} \setminus I = \{i_1, \dots, i_{m-1}\}.$$

We obtain from (7) that

$$(8) \qquad \sum_{i \notin I} a_i \binom{n-i}{j} \xi^{n-i} = -\binom{n}{j} \xi^n - \sum_{i \in I} a_i \binom{n-i}{j} \xi^{n-i} \quad (0 \le j < m).$$

The solvability of this system of linear equations in $a_i \xi^{n-i}$ ($i \notin I$) implies that the following matrix (b_{rs}) is singular

$$b_{rs} = \begin{cases} \binom{n-i_s}{r-1} & \text{if} \quad 1 \le r \le m, \ 1 \le s < m, \\ \binom{n}{r-1} \xi^n + \sum_{i \in I} a_i \binom{n-i}{r-1} \xi^{n-i} & \text{if} \quad 1 \le r \le m, \ s = m. \end{cases}$$

The equality $\det(b_{rs}) = 0$ implies by Lemma 2, on omitting a double product which is clearly different from zero, that

$$\xi^n \prod_{s=1}^{m-1} i_s + \sum_{i\in I} a_i \xi^{n-i} \prod_{s=1}^{m-1} (i_s - i) = 0.$$

Hence ξ is determined up to n possibilities and then the system (8) determines a_i $(i \notin I)$. □

Proof of Theorem 3. Let τ_i $(i = 1, \dots, n)$ be the i-th fundamental symmetric function of $x_1, \dots, x_n$. We have by (1) that

$$(-1)^i a_i = \tau_i(\underbrace{\xi_1, \dots, \xi_1}_{n_1}, \underbrace{\xi_2, \dots, \xi_2}_{n_2}, \dots, \underbrace{\xi_k, \dots, \xi_k}_{n_k}) \quad (1 \le i \le k).$$

By the Newton formulae we obtain

$$b_i = \sigma_i(\underbrace{\xi_1, \dots, \xi_1}_{n_1}, \underbrace{\xi_2, \dots, \xi_2}_{n_2}, \dots, \underbrace{\xi_k, \dots, \xi_k}_{n_k}) \quad (1 \le i \le k),$$

where σ_i is the sum of i-th powers and the b_i are uniquely determined by the a_i $(1 \le i \le k)$. Thus setting

$$f_i(x_1, \dots, x_k) = \sum_{j=1}^{k} n_j x_j^i \quad (1 \le i \le k)$$

we obtain the system of equations

$$b_i = f_i(\xi_1, \dots, \xi_k) \quad (1 \le i \le k). \tag{9}$$

The Jacobian

$$\det\left(\frac{\partial f_i}{\partial x_j}(\xi_1, \dots, \xi_n)\right)_{\substack{i=1,\dots,k \\ j=1,\dots,k}} = k! \prod_{j=1}^{k} n_j \prod_{1\le i<j\le k} (\xi_j - \xi_i) \ne 0,$$

hence the system (9) has only finitely many solutions in distinct $\xi_1, \dots, \xi_k$ and by Bézout theorem, the number of solutions is at most $k!$ (cf. the Lemma in [5]). Hence there are at most $k!$ possibilities for $f(x)$. □

Proof of Theorem 4. If the degree n of f is ≤ 4, then the statement follows from Theorems 1 and 2. Suppose that $n = 5$. Then, using again Theorems 1 and 2, we may assume that f has exactly three zeros, of multiplicities $2, 2, 1$, respectively. By a similar consideration, for $n = 6$ we obtain that either f has exactly three zeros, of multiplicities $2, 2, 2$ or $3, 2, 1$, respectively, or f has exactly four zeros of multiplicities $2, 2, 1, 1$, respectively. We give the proof only for $n = 5$, the cases when $n = 6$ can be treated similarly.

Let the three zeros of f be ξ_1, ξ_2, ξ_3, of multiplicities $2, 2, 1$, respectively. Then, by factoring in $K[x]$, we can write

$$f(x) = x^5 + a_1 x^4 + a_2 x^3 + a_3 x^2 + a_4 x + a_5 = (x + b_1)(x^2 + b_2 x + b_3)^2, \tag{10}$$

with some $b_1, b_2, b_3 \in K$. (This step is important from the computational point of view.) We show that by fixing any three of the coefficients a_i $(i = 1, \dots, 5)$, there are only finitely many possibilities for the b_j $(j = 1, 2, 3)$, whence for ξ_1, ξ_2, ξ_3. We consider only the case when a_1, a_3 and a_5 are fixed, the proof is similar in the other cases.

By expanding (10), we get the system of equations

$$(11) \qquad b_1 + 2b_2 - a_1 = 0, \quad b_1 b_2^2 + 2b_1 b_3 + 2b_2 b_3 - a_3 = 0, \quad b_1 b_3^2 - a_5 = 0.$$

Taking the resultants of the first and second, and first and third of these equations with respect to b_1, we get

$$(12) \qquad -2b_2^3 + a_1 b_2^2 - 2b_2 b_3 + 2a_1 b_3 - a_3 = 0 \quad \text{and} \quad -2b_2 b_3^2 + a_1 b_3^2 - a_5 = 0.$$

Now taking the resultant of these two equations with respect to b_2, we obtain

$$8a_1 b_3^7 - 8a_3 b_3^6 + 8a_5 b_3^5 + 2a_1^2 a_5 b_3^4 - 4a_1 a_5^2 b_3^2 + 2a_5^3 = 0.$$

By our assumption $a_1 \neq 0$. Hence there are at most 7 possibilities for b_3. By the third equation of (11), as $a_5 \neq 0$, we have $b_3 \neq 0$. Hence, using the second equation of (12), b_2 is determined by the choice of b_3. Now the third equation of (11) gives that b_1 is also determined.

By a similar argument, and a tedious computation we get in every case that the b_j $(j = 1, 2, 3)$ are determined up to finitely many possibilities. As we come to a similar conclusion also when $n = 6$, the theorem follows. $\square$

Proof of Theorem 5. If all the multiplicities of the zeros of f are divisible by l, then f is an l-th power in $\mathbb{Q}[x]$, and the statement is trivial. Suppose that f has exactly one zero of multiplicity not divisible by l. Then we can write

$$f(x) = x^n + a_1 x^{n-1} + \dots + a_n = (x + t)^k (x^m + b_1 x^{m-1} + \dots + b_m)^l,$$

with $1 \leq k < l$, and with some $t, b_1, \dots, b_m \in \mathbb{Q}$. We put $z = 1/x$ to obtain

$$1 + a_1 z + \dots + a_n z^n = (1 + tz)^k (1 + b_1 z + \dots + b_m z^m)^l,$$

whence

$$(13) \qquad \sqrt[l]{\frac{1 + a_1 z + \dots + a_n z^n}{(1 + tz)^k}} = 1 + b_1 z + \dots + b_m z^m.$$

We consider (13) as an equation concerning (real) generating functions (in z) of certain series. Set

$$(14) \qquad \sqrt[l]{1 + a_1 z + \dots + a_n z^n} = \sum_{i=0}^{\infty} c_i z^i.$$

Without loss of generality we may assume that $c_0 = 1$, whence $c_i \in \mathbb{Q}$ for $i \in \mathbb{N}$. Moreover, by differentiation we get for all $i \geq 1$ that c_i is linear in a_i, and c_j does not depend on a_i when $0 \leq j < i$. On the other hand, a simple calculation gives

$$(1 + tz)^{-k/l} = \sum_{i=0}^{\infty} s_i t^i z^i,$$

with

$$s_i = \left(-\frac{1}{l}\right)^i \frac{\prod_{j=0}^{i-1}(k+jl)}{i!} \quad (i = 0, 1, 2, \ldots).$$

Comparing the coefficients of z^{m+1} on the left- and right hand side of (13) and using the facts that $c_0 = 1$, that $c_1, \ldots, c_m$ are uniquely determined, and that $s_1, \ldots, s_m, s_{m+1}$ are known and $s_{m+1} \neq 0$, we obtain that t is a zero of a polynomial of degree $m+1$ with rational coefficients. After fixing t, the coefficients b_r $(1 \leq r \leq m)$ are uniquely determined by (13). As $m = [(n-1)/l] = (n-k)/l$, the theorem follows. □

Proof of the Proposition. From the course of the proof of Theorem 5, the statement i) is clear. To prove the statement ii), we use that in (14) for every $i \in \{1, \ldots, n\}$, c_i is linear in a_i, and c_j does not depend on a_i when $0 \leq j < i$. Hence fixing the coefficients a_i for $i = 1, \ldots, m+1$ successively, it is easy to see that the polynomial of degree $m+1$ determining t can have $m+1$ distinct rational zeros. Thus we may obtain $m+1$ different values for t. Hence, as $a_1, \ldots, a_{m+1}$ are fixed, by (13) we get also $m+1$ different values for $(b_1, \ldots, b_m)$ and for $(a_{m+2}, \ldots, a_n)$. □

To prove Theorem 6, we need some lemmas.

Lemma 3. *Let $t_1, t_2, \alpha \in \mathbb{R}$. Put $p(z) = 1 - t_1 z + t_2 z^2$ and $q(z) = (p(z))^\alpha$. Then for every non-negative integer r we have*

$$q^{(r)}(z) = \sum_{i=0}^{[r/2]} \frac{t_2^i r! \prod_{j=0}^{r-i-1}(\alpha - j)}{i!(r-2i)!} (p(z))^{\alpha - r + i} (p'(z))^{r-2i},$$

where $q^{(r)}$ denotes the r-th derivative of q.

Proof. We proceed by induction on r. One can easily check the statement for $r = 0$. Write

$$c(i, r) = \frac{t_2^i r! \prod_{j=0}^{r-i-1}(\alpha - j)}{i!(r-2i)!}$$

for $r \geq 0$ and $0 \leq i \leq [r/2]$, and suppose that the lemma is true for some r. Then we have

$$q^{(r+1)}(z) = \left(\sum_{i=0}^{[r/2]} c(i, r)(p(z))^{\alpha - r + i}(p'(z))^{r-2i} \right)'.$$

Thus to prove the statement, it is sufficient to verify that

$$(\alpha - r)c(0, r) = c(0, r+1),$$

$$2t_2(r - 2(i-1))c(i-1, r) + (\alpha - r + i)c(i, r) = c(i, r+1) \quad \text{for} \quad i = 1, \ldots, [r/2],$$

and

$$2t_2(r - 2[r/2])c([r/2], r) = \begin{cases} 0, & \text{if } r \text{ is even}, \\ c([(r+1)/2], r+1), & \text{if } r \text{ is odd}. \end{cases}$$

However, these equalities can be checked by a simple calculation, and the lemma follows. □

If h is any positive integer, then as usual, we put $(2h-1)!! = \prod_{i=1}^{h}(2i-1)$.

Lemma 4. *Let t_1, t_2 be arbitrary rationals, and let $G_r(t_1,t_2)$ $(r = 0,1,2,\dots)$ be the sequence having the generating function $(1-t_1z+t_2z^2)^{-1/2}$ in z, with $G_0(t_1,t_2) = 1$. Then for every r we have*

$$G_r(t_1,t_2) = \sum_{i=0}^{[r/2]} \frac{(-1)^i(2(r-i)-1)!!}{2^{r-i}i!(r-2i)!} t_1^{r-2i}t_2^i.$$

Proof. Put $p(z) = 1 - t_1z + t_2z^2$ and $\alpha = -1/2$. By $p(0) = 1$ and $p'(0) = -t_1$, the statement easily follows from Lemma 3. □

Remark 3. It is well-known (see e.g. [3] p. 10) that the generating function of the Dickson polynomials of the second kind

$$u_r(t_1,t_2) = \sum_{i=0}^{[r/2]} \binom{r-i}{i} t_1^{r-2i}t_2^i$$

is given by $(1-t_1z+t_2z^2)^{-1}$ (in z). Hence the above polynomials $G_r(t_1,t_2)$ are closely related to the Dickson polynomials.

Lemma 5. *The polynomials $G_r(t_1,t_2)$ defined in Lemma 4, for $r \geq 0$ satisfy the recursive formula*

$$G_{r+2}(t_1,t_2) = \frac{2r+3}{2r+4}t_1G_{r+1}(t_1,t_2) - \frac{r+1}{r+2}t_2G_r(t_1,t_2).$$

Proof. Using the explicit forms of the polynomials $G_r(t_1,t_2)$ given in Lemma 4, the statement can be easily checked by induction. □

In what follows, the resultant of $T_1, T_2 \in \mathbb{Q}[u,v]$ with respect to v will be denoted by $\mathrm{Res}_v(T_1,T_2)$.

Lemma 6. *Let d be a non-negative integer, and let $P, Q \in \mathbb{Q}[u,v]$ be given by*

$$P(u,v) = \sum_{i=0}^{[d/2]} p_iu^{d-2i}v^i \quad \text{and} \quad Q(u,v) = \sum_{i=0}^{[(d+1)/2]} q_iu^{d+1-2i}v^i.$$

Then $\mathrm{Res}_v(P,Q)$ is either identically zero, or it is a monomial of degree $d(d+1)/2$ in u.

Proof. We prove the statement only for d even, the case when d is odd can be treated in a similar way. For d even the resultant $\mathrm{Res}_v(P,Q)$ is a constant multiple of the determinant

$$\begin{vmatrix}
p_{\frac{d}{2}} & p_{\frac{d-2}{2}}u^2 & p_{\frac{d-4}{2}}u^4 & \dots & p_0u^d & 0 & 0 & 0 & \dots & 0 \\
0 & p_{\frac{d}{2}} & p_{\frac{d-2}{2}}u^2 & p_{\frac{d-4}{2}}u^4 & \dots & p_0u^d & 0 & 0 & \dots & 0 \\
0 & 0 & p_{\frac{d}{2}} & p_{\frac{d-2}{2}}u^2 & p_{\frac{d-4}{2}}u^4 & \dots & p_0u^d & 0 & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \dots & 0 & p_{\frac{d}{2}} & p_{\frac{d-2}{2}}u^2 & p_{\frac{d-4}{2}}u^4 & \dots & p_0u^d \\
q_{\frac{d}{2}}u & q_{\frac{d-2}{2}}u^3 & q_{\frac{d-4}{2}}u^5 & \dots & q_0u^{d+1} & 0 & 0 & 0 & \dots & 0 \\
0 & q_{\frac{d}{2}}u & q_{\frac{d-2}{2}}u^3 & q_{\frac{d-4}{2}}u^5 & \dots & q_0u^{d+1} & 0 & 0 & \dots & 0 \\
0 & 0 & q_{\frac{d}{2}}u & q_{\frac{d-2}{2}}u^3 & q_{\frac{d-4}{2}}u^5 & \dots & q_0u^{d+1} & 0 & \dots & 0 \\
\vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\
0 & 0 & 0 & \dots & 0 & q_{\frac{d}{2}}u & q_{\frac{d-2}{2}}u^3 & q_{\frac{d-4}{2}}u^5 & \dots & q_0u^{d+1}
\end{vmatrix}$$

of size $d \times d$. Multiply each row of the above determinant by an appropriate power of u such that for every r with $1 \le r \le d$, in each entry of the r-th column the exponents of u become $2r-1$. To obtain this form, we have to multiply the determinant by $u^{\frac{d(d-1)}{2}}$ altogether. Then again for every $1 \le r \le d$, we take out u^{2r-1} from the r-th column. Altogether we take out u^{d^2}. After this process we obtain that the original determinant is just a constant multiple of $u^{\frac{d(d+1)}{2}}$, and the lemma is proved. □

Proof of Theorem 6. Suppose that f has at most two zeros of odd multiplicities. By Theorem 5 we may assume that n is even and f has exactly two zeros of odd multiplicities. In this case f can be written in the form

$$f(x) = x^n + a_1x^{n-1} + \ldots + a_n = (x^2 - t_1x + t_2)(x^m + b_1x^{m-1} + \ldots + b_{m-1}x + b_m)^2$$

where $n = 2m+2$, with some rational numbers $t_1, t_2, b_1, \ldots, b_m$. Put $z = 1/x$ to obtain

$$1 + a_1z + \ldots + a_nz^n = (1 - t_1z + t_2z^2)(1 + b_1z + \ldots + b_mz^m)^2,$$

which yields

$$\sqrt{\frac{1 + a_1z + \ldots + a_nz^n}{1 - t_1z + t_2z^2}} = 1 + b_1z + \ldots + b_mz^m. \tag{15}$$

We consider (15) as an equation of (real) generating functions (in z) of certain series. Set

$$\sqrt{1 + a_1z + \ldots + a_nz^n} = \sum_{i=0}^{\infty} c_iz^i.$$

Without loss of generality we may assume that $c_0 = 1$, whence $c_i \in \mathbb{Q}$ for every $i \in \mathbb{N}$. Lemma 4 gives

$$(1 - t_1z + t_2z^2)^{-1/2} = \sum_{r=0}^{\infty}\left(\sum_{i=0}^{[r/2]} \frac{(-1)^i(2(r-i)-1)!!}{2^{r-i}i!(r-2i)!}t_1^{r-2i}t_2^i\right)z^r.$$

Put

$$G_r(u,v) = \sum_{i=0}^{[r/2]} \frac{(-1)^i(2(r-i)-1)!!}{2^{r-i}i!(r-2i)!}u^{r-2i}v^i \quad (r \in \mathbb{N}),$$

and let

$$H_1(u,v) = \sum_{i=0}^{m+1} c_{m+1-i}G_i(u,v), \quad H_2(u,v) = \sum_{i=0}^{m+2} c_{m+2-i}G_i(u,v).$$

As $H_1(t_1,t_2)$ and $H_2(t_1,t_2)$ are just the coefficients of z^{m+1} and z^{m+2} on the left hand side of (15), respectively, we have $H_1(t_1,t_2) = H_2(t_1,t_2) = 0$. Let

$$H(u) = \mathrm{Res}_v(H_1(u,v), H_2(u,v))$$

and

$$G(u) = \mathrm{Res}_v(G_{m+1}(u,v), G_{m+2}(u,v)).$$

Using $c_0 = 1$ and the determinant form of the resultant, we see that the coefficients L_H and L_G of $u^{\frac{(m+1)(m+2)}{2}}$ (the highest power of u that could occur) in $H(u)$ and in $G(u)$, respectively, are equal.

We now prove that $L_G \neq 0$. Lemma 6 implies that $G(u)$ is either identically zero, or it is a monomial of degree $(m+1)(m+2)/2$. Thus

$$L_G = 0 \iff G(u) \equiv 0.$$

However, combining Lemma 5 with the fact that

$$\mathrm{Res}_v(G_1, G_2) = (1/2)u,$$

we get by induction that $\mathrm{Res}_v(G_{m+1}, G_{m+2}) \not\equiv 0$. Hence $L_H = L_G \neq 0$. Thus t_1 is a zero of the non-zero polynomial $H(u)$ of degree $(m+1)(m+2)/2$. Having such a t_1, we substitute it into $H_1(u,v)$ or $H_2(u,v)$, according to that $m+1$ or $m+2$ is even. In this way we obtain a polynomial of degree at most $[(m+2)/2]$, such that t_2 must be a zero of it. Thus there are at most $[(m+2)/2](m+1)(m+2)/2$ possible pairs (t_1, t_2). As for any fixed (t_1, t_2) the coefficients $b_1, \ldots, b_m$ are uniquely determined by (15), the theorem follows. □

We need the following lemma to prove our Corollary. This result is a simple consequence of a theorem of Brindza (see [1]).

Lemma 7. *Let b and l be integers with $l \geq 2$, and $F \in \mathbb{Q}[x]$ a polynomial. Let $\alpha_1, \ldots, \alpha_r$ be the zeros of F, and denote by h_i the multiplicity of α_i $(i = 1, \ldots, r)$. Put $q_i = l/gcd(l, h_i)$ $(i = 1, \ldots, r)$. Suppose that $(q_1, \ldots, q_r)$ is not a permutation of either of the r-tuples $(q, 1, 1, \ldots, 1)$ and $(2, 2, 1, 1, \ldots, 1)$. Then the equation*

$$F(x) = by^l$$

has only finitely many solutions $x, y \in \mathbb{Z}$, and these solutions can be effectively determined.

Proof of the Corollary. By Theorems 5 and 6, there are at most N polynomials $g(x) \in \mathbb{Q}[x]$ of degrees less than $n - m - \varepsilon$, for which the polynomial $f(x) + g(x)$ has at most ε zeros of multiplicities not divisible by l. Moreover, the exceptional polynomials $g(x)$ can be effectively determined. Thus the statement follows from Lemma 7. □

4. Acknowledgments

The authors are grateful to the referee for his/her useful and helpful remarks.

References

[1] B. Brindza, *On S-integral solutions of the equation $y^m = f(x)$*, Acta Math. Hung. **44** (1984), 133–139.

[2] K. Győry and Á. Pintér, *On the equation $1^k + 2^k + \ldots + x^k = y^n$*, Publ. Math. Debrecen **62** (2003), 403–414.

[3] R. Lidl, G. L. Mullen and G. Turnwald, *Dickson polynomials*, Longman Scientific & Technical, 1993.

[4] Á. Pintér, *On the number of simple zeroes of certain polynomials*, Publ. Math. Debrecen **42** (1993), 329–332.

[5] A. Schinzel, *On sums of roots of unity. Solution of two problems of R. M. Robinson*, Acta Arith. **11** (1966), 419–432.

[6] A. Schinzel, *On the greatest common divisor of two univariate polynomials I*, In: "A panorama of number theory or a view from Baker's garden", Cambridge University Press, Cambridge, 2002, pp. 337–352.

[7] M. Voorhoeve, K. Győry and R. Tijdeman, *On the Diophantine equation* $1^k + 2^k + \ldots + x^k + R(x) = y^z$, Acta Math. **143** (1979), 1–8.

Kálmán Győry
Lajos Hajdu
Ákos Pintér
Number Theory Research Group
of the Hungarian Academy of Sciences, and
University of Debrecen
Institute of Mathematics
P.O. Box 12
H-4010 Debrecen
Hungary

Andrzej Schinzel
Institute of Mathematics
of the Polish Academy of Sciences
ul. Śniadeckich 8.
P.O. Box 21
00-956 Warszawa 10
Poland

E-mail address:
gyory@math.klte.hu
hajdul@math.klte.hu
apinter@math.klte.hu
schinzel@impan.gov.pl