ON POLYNOMIALS WITH ONLY RATIONAL ROOTS

LAJOS HAJDU, ROBERT TIJDEMAN, AND NÓRA VARGA

Abstract. In this paper we study upper bounds for the degrees of polynomials with only rational roots. First we assume that the coefficients are bounded. In the second theorem we suppose that the primes 2 and 3 do not divide any coefficient. The third theorem concerns the case that all coefficients are composed of primes from a fixed finite set.

1. Introduction

Polynomials in $\mathbb{Z}[x]$ with only rational roots are the simplest examples of decomposable polynomials and forms. Such polynomials play an important role in the theory of Diophantine equations, see e.g. Ch. 9 of Evertse and Győry [11]. They cover norm forms which are crucial in Schmidt's Subspace Theorem [22], and index forms and discriminant forms, see Evertse and Győry [12]. Many papers on Diophantine equations deal with polynomials in $\mathbb{Z}[x]$ with only rational roots themselves, see e.g. Section 2 of Hajdu and Tijdeman [15].

There is also an extensive literature on polynomials with restricted coefficients, in particular, with coefficients belonging to one of the sets $\{-1,1\}, \{0,1\}$ or $\{-1,0,1\}$, see Hare and Jankauskas [18] and the references there. In the first case the polynomials are called Littlewood polynomials, in the second case (assuming that the constant term is non-zero) Newman polynomials. For examples of studies of the location of the roots of such polynomials, see Borwein et al. [4] and Berend and Golan [2] for Littlewood polynomials, Odlyzko and Poonen [21] and Mercer [20] for Newman polynomials, and Borwein and Pinner [7], Borwein and Erdélyi [5] and Drungilas and Dubickas [8] for polynomials with all coefficients in $\{-1,0,1\}$.

The set of polynomials $f(x) \in \mathbb{Z}[x]$ with all coefficients in $\{-1,0,1\}$, constant term non-zero and only rational roots is very restricted as

Date: April 25, 2023.

2020 *Mathematics Subject Classification.* 11R09.

Key words and phrases. Polynomials with restricted coefficients.

Research supported in part by the Eötvös Loránd Research Network (ELKH) and by the NKFIH grants 128088 and 130909.

can be simply checked: The only possible roots are 1 and -1. Hence $f(x) = \pm(x-1)^a(x+1)^b$ for some $a, b \in \mathbb{Z}_{\geq 0}$. The coefficient of x is $\pm(b-a)$. Therefore $|b-a| \leq 1$. It follows that $f(x) = \pm(x^2-1)^k$ maybe multiplied with either $x-1$ or $x+1$ where $k = \min(a, b)$. Since the coefficients of f are in $\{-1, 0, 1\}$, we obtain $k \in \{0, 1\}$ and the degree of f is at most 3. An example of such a polynomial of degree 3 is

$$f(x) = x^3 - x^2 - x + 1 = (x-1)^2(x+1). \tag{1}$$

In this paper we generalize this result in two ways. In the first place we require that the coefficients of f are bounded. By the height of a polynomial with integer coefficients we mean the maximum of the absolute values of its coefficients. We prove the following result.

Theorem 1.1. *Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree n with only non-zero rational roots and height bounded by $H \geq 2$. Then we have both*

$$n \leq \left(\frac{2}{\log 2} + o(1)\right) \log H \qquad (H \to \infty) \tag{2}$$

and

$$n \leq \frac{5}{\log 2} \log H. \tag{3}$$

Further, the constants $2/\log 2$ and $5/\log 2$ in (2) and (3), respectively, are best possible.

Remark 1. Observe that for any $f \in \mathbb{Z}[x]$ of degree n, the height of $g := x^m f(x)$ is the same as that of f, while $\deg(g) = m + n$. So the assumption that the roots of f are non-zero is clearly necessary.

The second generalization concerns the case that none of the coefficients of $f(x)$ is divisible by 2 or 3. We prove

Theorem 1.2. *Every polynomial $f(x) \in \mathbb{Z}[x]$ with only rational roots of which no coefficient is divisible by 2 or 3 has degree at most 3.*

Remark 2. Example (1) shows that degree 3 is possible.

A further restriction is that the coefficients of f are integral S-units, that is integers composed of primes from a finite set S. Such polynomials are called S-polynomials. The next theorem shows that for any n there are only finitely many families of S-polynomials of degree n having only rational roots.

Theorem 1.3. *Let S be a finite set of primes with $|S| = s$ and n a positive integer. There exists an explicitly computable constant $C =$*

$C(n,s)$ depending only on n and s and sets T_1, T_2 with $\max(|T_1|,|T_2|) \le$ *C of n-tuples of S-units and $(n-1)/2$-tuples of S-units for n odd, respectively, such that if $f(x)$ is an S-polynomial of degree n having only rational roots $q_1, \dots q_n$, then $q_1, \dots, q_n$ satisfy one of the conditions* (i) *or* (ii)*:*

(i) *$(q_1, \dots, q_n) = u(r_1, \dots, r_n)$ with some $(r_1, \dots, r_n) \in T_1$ and S-unit u,*

(ii) *$n = 2t+1$ is odd, and re-indexing $q_1, \dots, q_n$ if necessary, we have $q_1 = u$ and $(q_2, \dots, q_n) = v(r_1, -r_1, \dots, r_t, -r_t)$ with some $(r_1, \dots, r_t) \in T_2$ and S-units u, v.*

Further, the possibilities (i) and (ii) cannot be excluded.

The proof of Theorem 1.1 is elementary. In the proof of Theorem 1.2 we use an old result of Fine [14] that if all the coefficients of the polynomial $(x+1)^n$ are odd, then n is of the form $2^\alpha - 1$ for some $\alpha \in \mathbb{Z}_{\ge 0}$. We derive a corresponding result for the prime 3 in place of 2. Its proof is elementary. The proof of Theorem 1.3 is based on an estimate of Amoroso and Viada [1] on the number of non-degenerate, non-proportional solutions of S-unit equations. We finish the paper with stating some open questions.

2. Proofs

Observe that the rational roots of an S-polynomial $f(x)$ are S-units, i.e. rational numbers whose numerators and denominators are composed exclusively of primes in S. This follows from the well-known fact that the denominator of a root of $f(x)$ divides the leading coefficient of $f(x)$, while its numerator divides the constant term of $f(x)$. In the sequel we shall use this fact without any further mentioning.

Proof of Theorem 1.1. On the one hand, let $f(x) = \sum_{j=0}^n a_j x^j$. Then

$$|f(\mathrm{i})| \le \left| \sum_{j \text{ is even}} |a_j| + \mathrm{i} \sum_{j \text{ is odd}} |a_j| \right| \le \sqrt{\frac{1}{2}n^2 + n + 1}\; H. \tag{4}$$

On the other hand, we may write $f(x) = \prod_{j=1}^n (q_j x - p_j)$ with $p_j, q_j \in \mathbb{Z}_{\neq 0}$ for all j. Then

$$|f(\mathrm{i})| = \left| \prod_{j=1}^n (q_j \mathrm{i} - p_j) \right| = \prod_{j=1}^n \sqrt{q_j^2 + p_j^2} \ge (\sqrt{2})^n. \tag{5}$$

Therefore,

$$n \log 2 \le \log\left(\frac{1}{2}n^2 + n + 1\right) + 2 \log H. \tag{6}$$

From this (2) easily follows. For the height H of the polynomial $f(x) = (x^2-1)^{n/2}$ with even $n \geq 2$ by Stirling's formula we have $\log H = (1+o(1))n\log 2/2$. This shows that the constant $2/\log 2$ in (2) is best possible.

To prove (3), observe that assuming $(5/\log 2)\log H < n$ from (6) we obtain

$$n\log 2 < \log\left(\frac{1}{2}n^2+n+1\right) + \frac{2n\log 2}{5}.$$

Hence we easily get

$$n \leq 9.$$

Further, observe that if we assume that f has a root different from ± 1, then (5) can be sharpened to

$$|f(\mathrm{i})| \geq \sqrt{5}(\sqrt{2})^{n-1}. \tag{7}$$

Thus, in this case combining $(5/\log 2)\log H < n$ with (4) and (7), we get a contradiction for $n \geq 1$. So to prove (3), we only need to check the polynomials of the shape $f(x) = \pm(x+1)^a(x-1)^{n-a}$ with $0 \leq a \leq n$ for $1 \leq n \leq 9$. A simple calculation gives that for all these polynomials (3) holds. In particular, for $n=5$ and $a=2,3$ we have equality. Thus e.g. the polynomial

$$(x-1)^3(x+1)^2 = x^5 - x^4 - 2x^3 + 2x^2 + x - 1$$

shows that the constant $5/\log 2$ in (3) is best possible. So the theorem is proved. $\square$

Remark 3. Several authors have considered upper bounds for the number r of real roots of $f(x) \in \mathbb{R}[x]$. Bloch and Pólya [3] proved

$$r \ll_H n\log\log n/\log n.$$

This was improved by E. Schmidt (unpublished) and further by Schur [23]. Schur proved

$$r^2 < 4n\log Q \quad \text{for } n > 6, \tag{8}$$

where

$$Q = \frac{1}{|a_0a_n|^{1/2}}(a_0^2+a_1^2+\cdots+a_n^2)^{1/2}.$$

Further he showed that the constant 4 in (8) cannot be improved. With $r=n$ we obtain for polynomials $f(x) \in \mathbb{Z}[x]$ with only real roots that

$$n \leq (4+o(1))\log H \qquad (H \to \infty). \tag{9}$$

(Here we used that $Q \leq \sqrt{n}\ H$ in this case.) By Theorem 1.1 the constant 4 in (9) cannot be replaced by a constant less than $2/\log 2 \sim$

2.885. For related results see Erdős and Turán [9], Littlewood and Offord [19], and Borwein, Erdélyi and Kós [6] too.

To prove Theorem 1.2, we need two lemmas. The first one is a direct consequence of Theorem 4 of Fine [14].

Lemma 2.1. *Let n be a positive integer such that all the coefficients of $(x+1)^n$ are odd. Then n is of the shape $2^\alpha - 1$ with some $\alpha \in \mathbb{Z}_{\geq 0}$.*

The next lemma is new, and provides a similar result for prime 3.

Lemma 2.2. *Let a, b be non-negative integers. Put $n := a+b$. If none of the coefficients of $(x-1)^a(x+1)^b$ is divisible by 3, then n is of the shape $3^\beta - 1, 2\cdot 3^\beta - 1, 3^\gamma + 3^\delta - 1$ or $2\cdot 3^\gamma + 3^\delta - 1$ with $\beta \geq 0, \gamma > \delta \geq 0$.*

Proof. We call a pair of non-negative integers (a, b) *good* if none of the coefficients of $f_{(a,b)}(x) := (x-1)^a(x+1)^b$ is divisible by 3; otherwise we say that (a, b) is *bad*. Observe that this property is symmetric in a and b in view of the substitution $x \to -x$. We distinguish between the residue classes of a and b modulo 3.

CASE $a \equiv \varepsilon \pmod 3$, $b \equiv 0 \pmod 3$, $\varepsilon \in \{0, 1\}$. Letting $a = 3u + \varepsilon$, $b = 3v$ we get that

$$f_{(a,b)}(x) \equiv (x^3 - 1)^u (x^3 + 1)^v (x - 1)^\varepsilon \pmod 3.$$

Hence (a, b) is good if and only if $u = v = 0$, i.e. $n = 0$ or 1.

CASE $b \equiv \varepsilon \pmod 3$, $a \equiv 0 \pmod 3$, $\varepsilon \in \{0, 1\}$. By symmetry, this yields the same conclusion as in the previous case.

CASE $a \equiv 2 \pmod 3$, $b \equiv 0 \pmod 3$. Writing $a = 3u + 2$, $b = 3v$ we see that

$$f_{(a,b)}(x) \equiv (x^3 - 1)^u (x^3 + 1)^v (x^2 + x + 1) \pmod 3.$$

This shows that (a, b) is good if and only if (u, v) is good.

CASE $b \equiv 2 \pmod 3$, $a \equiv 0 \pmod 3$. By symmetry, this yields the same conclusion as in the previous case.

CASE $a \equiv b \equiv \varepsilon \pmod 3, \varepsilon \in \{1, 2\}$. Putting $a = 3u + \varepsilon$, $b = 3v + \varepsilon$ we see that

$$f_{(a,b)}(x) \equiv (x^3 - 1)^u (x^3 + 1)^v (x^2 - 1)^\varepsilon \pmod 3.$$

Hence (a, b) is bad, as the coefficient of x will be $0 \pmod 3$.

CASE $a \equiv 2 \pmod 3$, $b \equiv 1 \pmod 3$. Letting $a = 3u + 2$, $b = 3v + 1$ we obtain that

$$f_{(a,b)}(x) \equiv (x^3 - 1)^u (x^3 + 1)^v (x^3 - x^2 - x + 1) \pmod 3. \tag{10}$$

From this we immediately see that if (u,v) is bad, then (a,b) is bad, too. Assume that (u,v) is good. Then we may write

$$(x^3-1)^u(x^3+1)^v=\sum_{i=0}^{u+v} c_i x^{3i} \tag{11}$$

with $3\nmid c_i$ $(i=0,\dots,u+v)$; in particular, $c_{u+v}=1$. Then, combining (10) and (11), we obtain that (a,b) is good if and only if none of the integers

$$c_{u+v},\ c_{u+v}+c_{u+v-1},\ \dots,\ c_1+c_0,c_0$$

is divisible by 3. Since $c_{u+v}=1$, this gives $c_i\equiv 1 \pmod 3$ $(i=0,\dots,u+v)$. Hence we obtain, on replacing x^3 by x_1 in (11), that every coefficient of $(x_1-1)^u(x_1+1)^v$ is $1 \pmod 3$. This is equivalent with

$$(x_1-1)^{u+1}(x_1+1)^v\equiv x_1^{u+v+1}-1 \pmod 3. \tag{12}$$

We show that (12) holds precisely for

$$(u,v)=(3^\ell-1,0),\ (3^\ell-1,3^\ell)\ (\ell\geq 0). \tag{13}$$

It is easy to check that (12) is valid for (u,v) given by (13). Assume that (12) holds for some (u,v) and write $u+1=3U+p$, $v=3V+q$ with $0\leq p,q\leq 2$ and $U,V\geq 0$. Then (12) can be rewritten as

$$(x_1^3-1)^U(x_1^3+1)^V(x_1-1)^p(x_1+1)^q\equiv x_1^{u+v+1}-1 \pmod 3.$$

Hence we get two possibilities. If $(p,q)\neq(0,0)$, then we must have $(p,q)=(1,0),(1,1)$ and $(U,V)=(0,0)$. So $(u,v)=(0,0),(0,1)$ belonging to (13) with $\ell=0$. If $(p,q)=(0,0)$ then we easily see that either $V=0$ or $U=V$ must be valid. Then (12) can be rewritten as

$$(x_1^3-1)^U\equiv x_1^{3U}-1 \pmod 3$$

or

$$(x_1^6-1)^U\equiv x_1^{6U}-1 \pmod 3,$$

respectively. These clearly hold if and only if U is a power of 3, and our claim follows. Altogether, we see that in this case (a,b) is good if and only if (u,v) is good and (13) holds.

CASE $b\equiv 2 \pmod 3$, $a\equiv 1 \pmod 3$. By symmetry, (a,b) is good if and only if setting $a=3u+1$ and $b=3v+2$, (u,v) is good and

$$(u,v)=(0,3^\ell-1),\ (3^\ell,3^\ell-1)\ (\ell\geq 0). \tag{14}$$

We conclude that (a,b) with $a+b=n>1$ is good if and only if writing $a=3u+i$, $b=3v+j$ with $0\leq i,j\leq 2$, (u,v) is good and ([$(a,b) \pmod 3$ equals $(2,0)$ or $(0,2)$] or [$(a,b)\equiv(2,1) \pmod 3$ and (13) holds] or [$(a,b)\equiv(1,2) \pmod 3$ and (14) holds]).

Suppose $(a,b) \equiv (2,1) \pmod 3$. Then by (13) we have two options. If $(u,v) = (3^\ell - 1, 0)$ $(\ell \geq 0)$ then we have $n = 3^{\ell+1} = 3^{\ell+1} + 3^0 - 1$ and we are done. If $(u,v) = (3^\ell - 1, 3^\ell)$ $(\ell \geq 0)$ then $n = 2\cdot 3^{\ell+1} = 2\cdot 3^{\ell+1} + 3^0 - 1$, and our claim follows. By symmetry the case $(a,b) \equiv (1,2) \pmod 3$ with (14) leads to the same values of n.

It remains to deal with the case $(a,b) \pmod 3$ equals $(2,0)$ or $(0,2)$. In both cases we have $n = a+b = 3u+3v+2$. Writing $u = 3u_1 + u_0$, $v = 3v_1 + v_0$ with $u_0, v_0 \in \{0,1,2\}$ we have, by the above conclusion:

(u,v) with $u+v > 1$ is good if and only if (u_1, v_1) is good and
$([(u,v) \pmod 3$ equals $(2,0)$ or $(0,2)]$ or
$[(u,v) \equiv (2,1) \pmod 3$ and (13) holds$]$ or
$[(u,v) \equiv (1,2) \pmod 3$ and (14) holds$])$,
where in (13) and (14) (u,v) is replaced with (u_1, v_1).

Thus, by induction, all possible degrees n are obtained by applying the substitution $n \to 3n+2$ a number of times on the possible starting values $0, 1, 3^\ell, 2\cdot 3^\ell$ for any non-negative integer ℓ. By applying the substitution k times we find $3^k - 1, 2\cdot 3^k - 1, 3^\ell + 3^k - 1, 2\cdot 3^\ell + 3^k - 1$, respectively, with $\ell > k$, for the only possible values of n. $\square$

Remark 4. For all the mentioned values in Lemma 2.2 there are polynomials without coefficients divisible by 3. We have modulo 3:

$$(x-1)^{3^\ell - 1} = (x-1)^{3^\ell}/(x-1) \equiv (x^{3^\ell} - 1)/(x-1) = x^{3^\ell - 1} + x^{3^\ell - 2} + \ldots + 1,$$

$$\begin{aligned}(x-1)^{2\cdot 3^\ell - 1} \equiv (x^{3^\ell} - 1)^2/(x-1) &= (x^{3^\ell - 1} + x^{3^\ell - 2} + \ldots + 1)(x^{3^\ell} - 1) = \\ &= x^{2\cdot 3^\ell - 1} + x^{2\cdot 3^\ell - 2} + \ldots + x^{3^\ell} - x^{3^\ell - 1} - x^{3^\ell - 2} - \ldots - 1,\end{aligned}$$

$$\begin{aligned}(x-1)^{3^\ell - 1}(x+1)^{3^\ell} &= (x-1)^{3^\ell}(x+1)^{3^\ell}/(x-1) \equiv (x^{3^\ell} - 1)(x^{3^\ell} + 1)/(x-1) \\ &= (x^{3^\ell - 1} + x^{3^\ell - 2} + \ldots + 1)(x^{3^\ell} + 1) = x^{2\cdot 3^\ell - 1} + x^{2\cdot 3^\ell - 2} + \ldots + 1.\end{aligned}$$

The first identity can be multiplied by $(x+1)^{3^k} \equiv x^{3^k} + 1$ for any k less than ℓ and yields the solutions

$$(3^\ell - 1, 0), (3^\ell - 1, 1), (3^\ell - 1, 3), \ldots, (3^\ell - 1, 3^{\ell - 1})$$

for $(\deg(x-1), \deg(x+1))$. This provides the total degrees $3^\ell - 1, 3^\ell + 3^k - 1$.

The second assertion provides the total degree $2\cdot 3^\ell - 1$. This degree is found in another way by the third formula.

The third identity can be multiplied by $(x+1)^{3^k} \equiv x^{3^k}+1$ for any k less than ℓ and yields the solutions

$$(3^\ell-1,3^\ell),(3^\ell-1,3^\ell+1),(3^\ell-1,3^\ell+3),\dots,(3^\ell-1,3^\ell+3^{\ell-1})$$

for $(\deg(x-1),\deg(x+1))$. This provides the total degrees $2\cdot 3^\ell-1$ and $2\cdot 3^\ell+3^k-1$.

Proof of Theorem 1.2. Let f be as in the statement. Since we argue modulo 2 and 3, and $2,3$ do not divide the leading coefficient of f, we may assume that f is monic. Since the roots of f are odd, Lemma 2.1 shows that $n+1$ is a power of 2. Further, since the roots of f are not divisible by 3, by Lemma 2.2 we get that $n+1$ is of the shape $3^\beta, 2\cdot 3^\beta, 3^\gamma+3^\delta$ or $2\cdot 3^\gamma+3^\delta$. The combination is possible only for $n=0,1,3$, as a simple check reveals. □

For the proof of Theorem 1.3 we use the theory of S-unit equations. Let S be a finite set of primes, $b_1,\dots,b_m$ non-zero rationals, and consider the equation

$$b_1x_1+\dots+b_mx_m=0 \quad \text{in } S\text{-units } x_1,\dots,x_m. \tag{15}$$

A solution $(y_1,\dots,y_m)$ of (15) is called non-degenerate if

$$\sum_{i\in I} b_iy_i \neq 0 \quad \text{for each non-empty subset } I \text{ of } \{1,\dots,m\}.$$

Further, two solutions $(y_1,\dots,y_m)$ and $(z_1,\dots,z_m)$ are called proportional, if there is an S-unit u such that $(z_1,\dots,z_m)=u(y_1,\dots,y_m)$. The following result is due to Amoroso and Viada; see the paragraph after (1.7) on p. 412 of [1]. (For an earlier version see [13], and for the case $m=2$ see [10].) Note that in fact the original result of Amoroso and Viada concerns the inhomogeneous case, i.e. where the right hand side of (15) is 1. However, it is easy to transform their result into the shape of (15).

Lemma 2.3. *Equation* (15) *has at most* $(8m-8)^{4(m-1)^4(m+s)}$ *non-degenerate, non-proportional solutions, where* $s=|S|$.

Proof of Theorem 1.3. Suppose that $f(x)=\sum_{j=0}^n a_jx^j$ is an S-polynomial of degree n having only rational roots $q_1,\dots,q_n$. By our assumption, $a_0,a_1,\dots,a_n$ are integral S-units. We have

$$A_j=\sigma_j(q_1,\dots,q_n) \quad (1\le j\le n) \tag{16}$$

where $A_j=(-1)^j a_{n-j}/a_n$ and σ_j is the j-th elementary symmetric polynomial (of degree j) of $q_1,\dots,q_n$. Using (16) for $j=1,2$ we get

$$q_1^2+\dots+q_n^2=A_1^2-2A_2. \tag{17}$$

This shows that $(q_1^2,\dots,q_n^2,A_1^2,A_2)$ yields a solution to the S-unit equation

$$x_1+\dots+x_n-x_{n+1}+2x_{n+2}=0. \tag{18}$$

If $(q_1^2,\dots,q_n^2,A_1^2,A_2)$ is a solution with no vanishing subsums, then by Lemma 2.3 we can write $q_i^2=u_0\ell_i$ $(i=1,\dots,n)$, where $(\ell_1,\dots,\ell_n)$ comes from a finite set of cardinality bounded in terms of n and s, and u_0 is an S-unit. Obviously, the squarefree parts of $\ell_1,\dots,\ell_n$ are the same, say ℓ_0. Thus letting $r_i^2=\ell_i/\ell_0$ $(i=1,\dots,n)$ and $u^2=u_0\ell_0$, we have $q_i=\pm ur_i$ $(i=1,\dots,n)$ and we are done in this case.

Hence we may assume that $(q_1^2,\dots,q_n^2,A_1^2,A_2)$ contains a vanishing subsum. Since $q_i^2>0$ $(1\le i\le n)$, the only possibility is that (after re-indexing $q_1,\dots,q_n$ if necessary) we have

$$q_1^2+\dots+q_k^2-A_1^2=0, \tag{19}$$

$$q_{k+1}^2+\dots+q_n^2+2A_2=0 \tag{20}$$

for some k with $1\le k<n$. It is easy to see that (19) and (20) do not have a vanishing subsum. Thus, similarly as above, Lemma 2.3 yields that

$$\begin{array}{rcl} (q_1,\dots,q_k) &=& u(w_1,\dots,w_k),\\ (q_{k+1},\dots,q_n) &=& v(r_1,\dots,r_\ell),\\ A_1=ut_1\neq 0, && A_2=v^2t_2\neq 0, \end{array}$$

where $\ell=n-k$ and both $(w_1,\dots,w_k,t_1)$ and $(r_1,\dots,r_\ell,t_2)$ come from finite sets of S-units of cardinalities bounded in terms of n and s, and u,v are S-units. Hence (16) for $j=1$ yields that

$$u(w_1+\dots+w_k)+v(r_1+\dots+r_\ell)=ut_1. \tag{21}$$

If $r_1+\dots+r_\ell\neq 0$ then the S-unit v/u comes from a set of cardinality bounded in terms of n and s, and we are in case (i). So we may suppose that

$$\begin{array}{rcl} w_1+\dots+w_k &=& t_1,\\ r_1+\dots+r_\ell &=& 0. \end{array}$$

As we have $k\ge 1$, $\ell\ge 1$ and, by (19) and (20),

$$\begin{array}{rcl} w_1^2+\dots+w_k^2-t_1^2 &=& 0,\\ r_1^2+\dots+r_\ell^2+2t_2 &=& 0, \end{array}$$

we obtain

$$\sigma_2(w_1,\dots,w_k)=0,\quad \sigma_2(r_1,\dots,r_\ell)=t_2.$$

We shall prove by contradiction that $k = 1$. Assume that $k \geq 2$. If $k = 2$ then $w_1 w_2 = 0$, which is not possible. So, $k \geq 3$. Hence

$$u^3\sigma_3(w_1, \dots, w_k) + u^2 v\sigma_2(w_1, \dots, w_k)\sigma_1(r_1, \dots, r_\ell)+ \\ + uv^2\sigma_1(w_1, \dots, w_k)\sigma_2(r_1, \dots, r_\ell) + v^3\sigma_3(r_1, \dots, r_\ell) - A_3 = 0.$$

Here $\sigma_j(r_1, \dots, r_\ell) = 0$ if $\ell < j$. In view of the previously obtained assertions, we get

$$u^3\sigma_3(w_1, \dots, w_k) + uv^2 t_1 t_2 + v^3\sigma_3(r_1, \dots, r_\ell) - A_3 = 0. \tag{22}$$

If $\sigma_3(w_1, \dots, w_k) \neq 0$ or $\sigma_3(r_1, \dots, r_\ell) \neq 0$ then (22) by Lemma 2.3 easily yields (both with or without vanishing subsums) that v/u belongs to a set of cardinality bounded in terms of n and s, and we are in case (i). So we may assume that

$$\sigma_3(w_1, \dots, w_k) = 0, \quad \sigma_3(r_1, \dots, r_\ell) = 0.$$

Then we get

$$w_1^3 + \dots + w_k^3 = \sigma_1(w_1, \dots, w_k)^3 - 3\sigma_1(w_1, \dots, w_k)\sigma_2(w_1, \dots, w_k)+ \\ + 3\sigma_3(w_1, \dots, w_k) = t_1^3.$$

We have obtained

$$\begin{cases} w_1 + \dots + w_k = t_1, \\ w_1^2 + \dots + w_k^2 = t_1^2, \\ w_1^3 + \dots + w_k^3 = t_1^3. \end{cases} \tag{23}$$

Note that (23) implies that there are indices i_1, i_2 with $w_{i_1} > 0$ and $w_{i_2} < 0$, thus

$$|t_1| = \sqrt{w_1^2 + \dots + w_k^2} = \sqrt{|w_1|^2 + \dots + |w_k|^2} \geq \\ \geq \sqrt[3]{|w_1|^3 + \dots + |w_k|^3} > |t_1|.$$

This contradiction shows that $k = 1$ and $\ell = n - 1$.

Recall that

$$\sigma_1(r_1, \dots, r_\ell) = 0, \quad \sigma_2(r_1, \dots, r_\ell) = t_2, \quad \sigma_3(r_1, \dots, r_\ell) = 0.$$

Hence (22) yields $A_3 = uv^2 t_1 t_2$. Further, by (16) and $k = 1$ we get

$$A_j = uv^{j-1} w_1 \sigma_{j-1}(r_1, \dots, r_\ell) + v^j \sigma_j(r_1, \dots, r_\ell) \quad (4 \leq j \leq n). \tag{24}$$

From this, taking $j = 4$ we obtain

$$\sigma_4(r_1, \dots, r_\ell) = A_4/v^4 \neq 0.$$

Now (24) for $j = 5$ by Lemma 2.3 yields that if $\sigma_5(r_1, \ldots, r_\ell) \neq 0$ then v/u comes from a set of cardinality bounded by n and s, and we are in case (i). So we may assume that

$$\sigma_5(r_1, \ldots, r_\ell) = 0.$$

Now by repeating this argument, we may assume that

$$\begin{cases} \sigma_j(r_1, \ldots, r_\ell) = A_j/v^j \neq 0 & \text{for } j \text{ even,} \\ \sigma_j(r_1, \ldots, r_\ell) = 0 & \text{for } j \text{ odd.} \end{cases}$$

In particular, since $\sigma_\ell(r_1, \ldots, r_\ell) = r_1 \cdots r_\ell$ cannot be zero, ℓ is even whence $n = \ell + 1$ is odd. Observing that $(x + r_1) \cdots (x + r_\ell)$ is an even polynomial, writing $\ell = 2t$ and re-indexing the S-units r_i $(1 \leq i \leq \ell)$ such that $r_{t+i} = -r_i$ $(1 \leq i \leq t)$, we see that we are in case (ii).

Finally, we show that the possibilities (i) and (ii) cannot be excluded. Indeed, if $r_1, \ldots, r_n$ is a set of rational roots of an S-polynomial of degree n, then clearly, the same is true for $ur_1, \ldots, ur_n$ for any S-unit u, showing the necessity of (i). On the other hand, let $r_1^2, \ldots, r_t^2$ be the rational roots of the S-polynomial $(x - r_1^2) \cdots (x - r_t^2)$. Then in the polynomial $(x^2 - r_1^2) \cdots (x^2 - r_t^2)$, all the coefficients of the even powers of x are S-units (while the coefficients of the odd powers of x equal 0). Thus for any S-units u, v, all the coefficients of the polynomial

$$(x + u)(x - vr_1)(x + vr_1) \cdots (x - vr_t)(x + vr_t)$$

are S-units. This shows that (ii) cannot be excluded either. Note that it is easy to construct as many such non-proportional tuples as we like: Take arbitrary tuples of n integers (or t squares) that are non-proportional and define S as the set of prime factors of the product of their elementary symmetric polynomials. □

3. Open problems

We wonder whether the following statement is correct:

Problem 1. *Is it true that for any primes p and q there exists an $n_1 = n_1(p, q)$ such that every polynomial $f(x) \in \mathbb{Z}[x]$ with only rational roots of which no coefficient is divisible by p or q has degree at most n_1?*

Theorem 1.1 shows that the answer is 'yes' for the pair of primes $(p, q) = (2, 3)$.

A weaker statement is a restriction to S-polynomials.

Problem 2. *Is it true that for any finite set S of primes there exists an $n_2 = n_2(S)$ such that every S-polynomial $f(x) \in \mathbb{Z}[x]$ with only rational roots has degree at most n_2?*

Theorem 1.2 yields an affirmative answer for sets S of primes with $2,3 \notin S$.

The last problem is raised by Lemmas 2.1 and 2.2.

Problem 3. *Is it true that for every prime p there exists a constant $c(p)$ such that if $f(x) \in \mathbb{Z}[x]$ has only rational roots and none of the coefficients of f is divisible by p, then* $\deg(f)+1$ *in its p-adic expansion has at most $c(p)$ non-zero digits? In particular, can one take $c(p) = p-1$?*

Lemmas 2.1 and 2.2 show that the answer is 'yes' with $c(p) = p-1$ for $p = 2,3$. Note that an affirmative answer to Problem 3 through a deep result of Stewart [24] would yield positive answers to Problems 1 and 2, as well.

Acknowledgements

The authors are grateful to the referee for the insightful and helpful remarks.

References

[1] F. Amoroso and E. Viada, *Small points on subvarieties of a torus*, Duke Math. J. **150** (2009), 407–442.

[2] D. Berend, Sh. Golan, *Littlewood polynomials with higher order zeros*, Math. Comput. **75** (2006), 1541–1552.

[3] A. Bloch, G. Pólya, *On the roots of certain algebraic equations*, Proc. London Math. Soc. **33** (1932), 102–114.

[4] P. Borwein, S. Choi, R. Ferguson, J. Jankauskas, *On Littlewood polynomials with prescribed number of zeros inside the unit disk*, Canad. J. Math. **67** (2015), 507–526.

[5] P. Borwein, T. Erdélyi, *On the zeros of polynomials with restricted coefficients*, Illinois J. Math. **41** (1997), 667–675.

[6] P. Borwein, T. Erdélyi, G. Kós, *Littlewood-type problems on* $[0,1]$, Proc. London Math. Soc. **79** (1999), 22–46.

[7] P. Borwein, C. Pinner, *Polynomials with* $\{0,+1,-1\}$ *coefficients and a root close to a given point*, Canad. J. Math. **49** (1997), 887–915.

[8] P. Drungilas, A. Dubickas, *Roots of polynomials of bounded height*, Rocky Mountain J. Math. **39** (2009), 527–543.

[9] P. Erdős, P. Turán, *On the distribution of roots of polynomials*, Ann. Math. **57** (1950), 105–119.

[10] J.-H. Evertse, *On equations in S-units and the Thue-Mahler equation*, Invent. Math. **78** (1984), 561–584.

[11] J.-H. Evertse, K. Győry, *Unit Equations in Diophantine Number Theory*, Cambridge Studies in Advanced Mathematics 146, Cambridge University Press, 2015.

[12] J.-H. Evertse, K. Győry, *Diophantine Equations in Diophantine Number Theory*, New Mathematical Monographs 32, Cambridge University Press, 2017.

[13] J.-H. Evertse, H. P. Schlickewei and W. M Schmidt, *Linear equations in variables which lie in a multiplicative group*, Ann. Math. **155** (2002), 807–836.

[14] N. J. Fine, *Binomial coefficients modulo a prime*, Amer. Math. Monthly 54 (1947), 589–592.

[15] L. Hajdu, R. Tijdeman, *The Diophantine equation* $f(x) = g(y)$ *for polynomials with simple rational roots*, submitted.

[16] L. Hajdu, R. Tijdeman, N. Varga, *Diophantine equations for Littlewood polynomials*, Acta Arith. (to appear).

[17] L. Hajdu, N. Varga, *Diophantine equations for polynomials with restricted coefficients,* I *(power values)*, Bull. Austral. Math. Soc. **106** (2022), 254–263.

[18] K.G. Hare, J. Jankauskas, *On Newman and Littlewood polynomials with prescribed number of zeros inside the unit disk*, Math. Comput. **90** (2021), 831–870.

[19] J.E. Littlewood, A.C. Offord, *On the number of real roots of a random algebraic equation.* II, Math. Proc. Cambridge Philos. Soc. **35** (1939), 133–148.

[20] I.D. Mercer, *Newman polynomials not vanishing on the unit circle*, Integers **12** (67) (2012), 7 pp.

[21] M. Odlyzko, B. Poonen, *Zeros of polynomials with* $0, 1$ *coefficients*, Enseign. Math. **39** (1993), 317–348.

[22] W.M. Schmidt, *Diophantine Approximations and Diophantine Equations*, Lect. Notes Math. 1467, Springer-Verlag, 1991.

[23] I. Schur, *Untersuchungen über algebraische Gleichungen*, Sitz. Preuss. Akad. Wiss., Phys.-Math. Kl. (1933), 403–428.

[24] C.L. Stewart, *On the representation of an integer in two different bases*, J. reine angew. Math **319** (1980), 63–72.

[25] G. Szegő, *Bemerkungen zu einem Satz von E. Schmidt über algebraische Gleichungen*, Sitz. Preuss. Akad. Wiss., Phys.-Math. Kl. (1934), 86–98.

Institute of Mathematics, University of Debrecen,
P. O. Box 400, H-4002 Debrecen, Hungary
and ELKH-DE Equations, Functions, Curves and their Applications Research Group
Email address: `hajdul@science.unideb.hu`

Mathematical Institute, Leiden University,
Postbus 9512, 2300 RA Leiden, The Netherlands
Email address: `tijdeman@ziggo.nl`

Institute of Mathematics, University of Debrecen,
P. O. Box 400, H-4002 Debrecen, Hungary
and ELKH-DE Equations, Functions, Curves and their Applications Research Group
Email address: `nvarga@science.unideb.hu`