Polynomials having only rational roots

L. Hajdu

University of Debrecen

Online seminar of the Number Theory Research Group

University of Debrecen

13 October 2023

Plan of the talk

- Introduction and motivation

- New results

  - sharp bounds for the degree in terms of the height
  - sharp bound for the degree if the coeffs are coprime to 6
  - finiteness and full description for fixed degree if the coeffs are composed of a fixed finite set of primes

- Open problems

The new results presented are joint with **R. Tijdeman** and **N. Varga**.

Introduction and motivation

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. results of **Evertse and Győry**.)

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 e.g. results concerning Littlewood polynomials and Newman polynomials.)

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. The degree of f is at most 3, an example is

$$f(x) = x^3 - x^2 - x + 1 = (x - 1)^2(x + 1).$$

Sharp bounds for the degree in terms of the height

Theorem 1 (Tijdeman, Varga, H. (2023))

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

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

and

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

Further, the constants $2/\log 2$ and $5/\log 2$ in (1) and (2), respectively, are best possible.

Sharp bounds for the degree in terms of the height

Remarks. 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.

Several authors have considered upper bounds for the number r of real roots of $f(x) \in \mathbb{R}[x]$. (See e.g. results of **Bloch and Pólya**, **E. Schmidt**, **Schur**, **Erdős and Turán**, **Littlewood and Offord**, **Borwein, Erdélyi and Kós**.)

For example, a result of **Schur** implies for polynomials $f(x) \in \mathbb{Z}[x]$ with only real roots that

$$n \leq (4 + o(1)) \log H \quad (H \to \infty).$$

Proof of Theorem 1

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

$$|f(\mathrm{i})| \leq \left| \sum_{j \text{ is even}} |a_j| + \mathrm{i} \sum_{j \text{ is odd}} |a_j| \right| \leq \sqrt{\frac{1}{2}n^2 + n + 1}\ H. \tag{3}$$

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

$$|f(\mathrm{i})| = \left| \prod_{j=1}^{n}(q_j\mathrm{i} - p_j) \right| = \prod_{j=1}^{n} \sqrt{q_j^2 + p_j^2} \geq (\sqrt{2})^n. \tag{4}$$

Therefore,

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

From this (1) easily follows.

Proof of Theorem 1

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 (1) is best possible.

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

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

whence $n \leq 9$.

These cases can be checked relatively easily, and (2) holds. In particular, 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 (2) is best possible.

Polynomials with coeffs coprime to 6

Theorem 2 (Tijdeman, Varga, H. (2023))

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.

The example

$$f(x) = x^3 - x^2 - x + 1 = (x-1)^2(x+1)$$

shows that degree 3 is possible.

Background of the proof of Theorem 2

The proof is based upon the following two lemmas.

Lemma 1 (Fine (1947))

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 $\alpha \in \mathbb{Z}_{\geq 0}$.

Lemma 2 (Tijdeman, Varga, H. (2023))

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 $\beta \geq 0, \gamma > \delta \geq 0$.

Remark. For all the mentioned values in Lemma 2 there are polynomials without coefficients divisible by 3.

Sketch of the proof of Lemma 2

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.

Sketch of the proof of Lemma 2

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

$$f_{(a,b)}(x) \equiv (x^3 - 1)^u (x^3 + 1)^v (x^3 - x^2 - x + 1) \pmod 3. \tag{6}$$

So if (u, v) is bad, then (a, b) is bad, too.

Assume that (u, v) is good. Then we may write

$$(x^3 - 1)^u (x^3 + 1)^v = \sum_{i=0}^{u+v} c_i x^{3i} \tag{7}$$

with $3 \nmid c_i$ $(i = 0, \dots, u + v)$; in particular, $c_{u+v} = 1$.

Then, combining (6) and (7), 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.

Sketch of the proof of Lemma 2

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 (7), that every coefficient of $(x_1 - 1)^u (x_1 + 1)^v$ is $1 \pmod 3$.

This is equivalent with

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

This holds precisely for $(u, v) = (3^\ell - 1, 0),\ (3^\ell - 1, 3^\ell)$ $(\ell \geq 0)$.

Background of the proof of Theorem 2

We may assume that f is monic.

Since the roots of f are odd, Lemma 1 shows that $n+1$ is a power of 2.

Further, since the roots of f are not divisible by 3, by Lemma 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 $n = 0, 1, 3$.

Polynomials with coeffs having only prime factors coming from a fixed finite set

Theorem 3 (Tijdeman, Varga, H. (2023))

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 $\max(|T_1|, |T_2|) \leq C$ 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.

Background of the proof of Theorem 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

$$b_1 x_1 + \cdots + b_m x_m = 0 \quad \text{in } S\text{-units } x_1, \dots, x_m. \tag{8}$$

A solution $(y_1, \dots, y_m)$ of (8) is called non-degenerate if

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

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 $(z_1, \dots, z_m) = u(y_1, \dots, y_m)$.

Lemma 3 (Amoroso and Viada (2009))

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

Sketch of the proof of Theorem 3

Write $f(x) = \sum_{j=0}^{n} a_j x^j$, 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

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

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 it for $j = 1, 2$ we get $q_1^2 + \cdots + q_n^2 = A_1^2 - 2A_2$.

This shows that $(q_1^2, \dots, q_n^2, A_1^2, A_2)$ yields a solution to the S-unit equation $x_1 + \cdots + x_n - x_{n+1} + 2x_{n+2} = 0$.

Sketch of the proof of Theorem 3

If $(q_1^2, \dots, q_n^2, A_1^2, A_2)$ is a solution with no vanishing subsums, then by Lemma 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 $q_i = \pm u r_i$ $(i = 1, \dots, n)$ and we are in case (i).

Hence we may assume that $(q_1^2, \dots, q_n^2, A_1^2, A_2)$ contains a vanishing subsum.

This case, with further careful analysis and delicate considerations lead to the statement by Lemma 3.

Sketch of the proof of Theorem 3

Finally, we show that the possibilities (i) and (ii) cannot be excluded.

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.

Open problems

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

Open problems

The last problem is raised by Lemmas 1 and 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 1 and 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** would yield positive answers to Problems 1 and 2, as well.

Thank you very much
for your attention!