On the irreducibility of polynomials that take a prime power value
by
A.I. BONCIOCAT, N.C. BONCIOCAT, AND A. ZAHARESCU

In memory of Laurențiu Panaitopol

Abstract

We provide several irreducibility criteria for polynomials with integer coefficients that take a prime power value and either have one large coefficient, or have all the coefficients of modulus 1. We also obtain upper bounds for the total number of irreducible factors of such polynomials, by studying their higher derivatives.

Key Words: Estimates for polynomial roots, prime power, irreducible polynomials.

2010 Mathematics Subject Classification: Primary 11C08; Secondary 11R09.

1 Introduction

Some classical irreducibility criteria rely on the existence of a suitable prime divisor of the value that a given polynomial takes at a specified integral argument. One of the most elegant results of this type, given by Pólya and Szegő in [12], is due to A. Cohn:

THEOREM A. If a prime number $p$ is expressed in the decimal system as $p = \sum_{i=0}^{n} a_i 10^i$ with $0 \leq a_i \leq 9$, then the polynomial $\sum_{i=0}^{n} a_i X^i$ is irreducible in $\mathbb{Z}[X]$.

This irreducibility criterion was generalized to an arbitrary base $b$ by Brillhart, Filaseta and Odlyzko [4]:

THEOREM B. If a prime number $p$ is expressed in the number system with base $b \geq 2$ as $p = \sum_{i=0}^{n} a_i b^i$, $0 \leq a_i \leq b-1$, then the polynomial $\sum_{i=0}^{n} a_i X^i$ is irreducible in $\mathbb{Z}[X]$. 

For several nice connections between prime numbers and irreducible polynomials, the reader is referred to Ram Murty [10] and Girstmair [8]. Murty [10] obtained an elementary proof of these irreducibility criteria, and also established an analogous result for polynomials with coefficients in $\mathbb{F}_q[t]$, with $\mathbb{F}_q$ a finite field. Inspired by these results, in [2] several irreducibility criteria are proved for integer polynomials that take a prime value and either have one large coefficient, or have all the coefficients of modulus 1. We mention here the following two:

**Theorem C.** If we write a prime number as a sum of integers $a_0, \ldots, a_n$ with $a_0a_n \neq 0$ and $|a_0| > \sum_{i=1}^{n} |a_i|^{2^i}$, then the polynomial $\sum_{i=0}^{n} a_i X^i$ is irreducible over $\mathbb{Q}$.

**Theorem D.** If all the coefficients of a polynomial $f$ are $\pm 1$ and $f(m)$ is a prime number for an integer $m$ with $|m| \geq 3$, then $f$ is irreducible over $\mathbb{Q}$.

Similar irreducibility criteria for multivariate polynomials over an arbitrary field have been obtained in [3]. One may naturally ask whether Cohn’s result will still hold true if we replace the prime number $p$ with $p^s$, $s \geq 2$. This is by no means necessarily true, as one can see by taking $p = 11$ and considering the polynomial $f(X)$ obtained by replacing the powers of 10 by the corresponding powers of $X$ in the decimal representation of $11^2$. In this case $f(10) = 121$, and the polynomial $f(X) = X^2 + 2X + 1$ is obviously reducible. For another example one may consider the decimal representation of $11^7$. Here $f(10) = 11^7 = 19487171$, and the polynomial $f(X)$ is also reducible, being divisible by $X + 1$.

The first aim of this paper is to find some additional conditions that guarantee us the irreducibility of a polynomial that takes a prime power value, and thus to complement the results in [2], by extending them to a larger class of polynomials. This will be achieved by adding a natural condition on the derivative of our polynomials. Our second goal is to derive upper bounds for the total number of irreducible factors of such polynomials, instead of irreducibility criteria, by considering their higher derivatives. Our first result extends Theorem B to prime powers, as follows.

**Theorem 1.1.** If a prime power $p^s$, $s \geq 2$ is expressed in the number system with base $b \geq 2$ as $p^s = \sum_{i=0}^{n} a_i b^i$, $0 \leq a_i \leq b - 1$ and $p \nmid \sum_{i=1}^{n} i a_i b^{i-1}$, then the polynomial $\sum_{i=0}^{n} a_i X^i$ is irreducible over $\mathbb{Q}$.

The following three results give irreducibility conditions for polynomials that have one coefficient of sufficiently large modulus and take a value divisible by a prime power $p^s$, $s \geq 2$.

**Theorem 1.2.** Let $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$, $a_0a_n \neq 0$. Suppose that $f(m) = p^s \cdot q$ for some integers $m, s, q$ and a prime number $p$, with $s \geq 2$, $p \nmid qf'(m)$ and

$$|a_0| > \sum_{i=1}^{n} |a_i| \cdot (|m| + |q|)^i.$$

Then $f$ is irreducible over $\mathbb{Q}$.
Then \( f \) is irreducible over \( \mathbb{Q} \).

**Theorem 1.4.** Let \( f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X] \), \( a_0 a_n \neq 0 \). Suppose that \( f(m) = p^s \cdot q \) for some integers \( m, s, q \) and a prime number \( p \), with \( s \geq 2 \), \( |m| > |q| \) and \( p \nmid qf'(m) \) and

\[
|a_n| > \sum_{i=0}^{n-1} |a_i| \cdot (|m| - |q|)^{i-n}.
\]

Then \( f \) is irreducible over \( \mathbb{Q} \).

Roughly speaking, the above three results show in particular that if \( f(m) \) is a prime power for an integer \( m \) with \( |m| \geq 2 \), \( f(m) \) and \( f'(m) \) are relatively prime, and \( f \) has one coefficient of sufficiently large modulus, then \( f \) must be irreducible over \( \mathbb{Q} \).

Moreover, from Theorems 1.2 and 1.4 one obtains the following irreducibility criteria, that extend Theorems C and D to polynomials that take a prime power value.

**Corollary 1.5.** If we write a prime power \( p^s \), \( s \geq 2 \), as a sum of integers \( a_0, \ldots, a_n \) with \( a_0 a_n \neq 0 \), \( |a_0| > \sum_{i=0}^{n} |a_i| 2^i \), and \( a_1 + 2a_2 + \cdots + a_n \) not divisible by \( p \), then the polynomial \( \sum_{i=0}^{n} a_i X^i \) is irreducible over \( \mathbb{Q} \).

**Corollary 1.6.** Let \( f \) be a Littlewood polynomial. If \( f(m) \) is a prime power \( p^s \), \( s \geq 2 \), for an integer \( m \) with \( |m| \geq 3 \), and \( p \nmid f'(m) \), then \( f \) is irreducible over \( \mathbb{Q} \).

As it was done in [2], we will also prove some related results, that depend on some suitable sets of parameters.

**Proposition 1.7.** Let \( f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X] \), with \( 0 = d_0 < d_1 < \cdots < d_n \) and \( a_0 a_1 \cdots a_n \neq 0 \). Suppose that \( f(m) = p^s \cdot q \) for some integers \( m, s, q \) and a prime number \( p \), with \( s \geq 2 \), \( p \nmid qf'(m) \), and let \( \mu_0 = 0, \mu_n = 1 \) and \( \mu_1, \ldots, \mu_{n-1} \) be arbitrary positive constants. If

\[
|m| - |q| > \max_{1 \leq j \leq n} \left\{ \frac{(1 + \mu_{j-1}) |a_{j-1}|}{\mu_j |a_j|} \right\}^{\frac{1}{j_j - j_{j-1}}},
\]

then \( f \) is irreducible over \( \mathbb{Q} \).
Proposition 1.8. Let \( f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X] \), with \( 0 = d_0 < d_1 < \cdots < d_n \) and \( a_0 a_1 \cdots a_n \neq 0 \). Suppose that \( f(m) = p^s \cdot q \) for some integers \( m, s, q \) and a prime number \( p \), with \( s \geq 2 \), \( p \nmid qf'(m) \), and let \( \mu_0 = 1, \mu_n = 0 \) and \( \mu_1, \ldots, \mu_{n-1} \) be arbitrary positive constants. If
\[
|m| + |q| < \min_{1 \leq j \leq n} \left\{ \frac{\mu_{j-1}|a_{j-1}|}{(1 + \mu_j)|a_j|} \right\}^{\frac{1}{d_j-1}},
\]
then \( f \) is irreducible over \( \mathbb{Q} \).

Proposition 1.9. Let \( f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X] \), with \( a_0 a_n \neq 0 \). Suppose that \( f(m) = p^s \cdot q \) for some integers \( m, s, q \) and a prime number \( p \), with \( s \geq 2 \), \( p \nmid qf'(m) \), and let \( \mu_0 = 0 \) and \( \mu_1, \ldots, \mu_n \) be arbitrary positive constants. If
\[
|m| - |q| > \max_{0 \leq j \leq n-1} \left\{ \frac{\mu_j}{\mu_1} \cdot \frac{\mu_n}{\mu_{j+1}} \cdot \frac{|a_j|}{|a_n|} \right\},
\]
then \( f \) is irreducible over \( \mathbb{Q} \).

Proposition 1.10. Let \( f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X] \), with \( a_0 a_n \neq 0 \). Suppose that \( f(m) = p^s \cdot q \) for some integers \( m, s, q \) and a prime number \( p \), with \( s \geq 2 \) and \( p \nmid qf'(m) \). Let \( \mu_0 = 0 \) and \( \mu_1, \ldots, \mu_n \) be arbitrary positive constants. If
\[
|m| - |q| > \max_{0 \leq j \leq n-1} \left\{ \frac{\mu_j}{\mu_1} \cdot \frac{\mu_n}{\mu_{j+1}} \cdot \frac{|a_j|}{|a_n|} \right\},
\]
then \( f \) is irreducible over \( \mathbb{Q} \).

In particular, for \( \mu_1 = \mu_2 = \ldots = \mu_n = 1 \) we obtain the following irreducibility criterion.

Corollary 1.11. Let \( f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X] \), with \( a_0 a_n \neq 0 \). Suppose that \( f(m) = p^s \cdot q \) for some integers \( m, s, q \) and a prime number \( p \), with \( s \geq 2 \) and \( p \nmid qf'(m) \). If
\[
|m| - |q| > \max \left\{ \frac{|a_0|}{|a_n|}, 1 + \frac{|a_1|}{|a_n|}, 1 + \frac{|a_2|}{|a_n|}, \ldots, 1 + \frac{|a_{n-1}|}{|a_n|} \right\},
\]
then \( f \) is irreducible over \( \mathbb{Q} \).

The above results are flexible and may be useful in certain applications where other irreducibility criteria fail. In order to keep this paper self-contained, we will give in Section 2 below detailed proofs, that employ the methods used in [2], [10] and [12], and we will also include the proofs given in [2] for the estimates on polynomial roots needed in our results. At the end of Section 2, in Lemma 2.3 we will give a method to obtain upper bounds for the total number of irreducible factors of a given polynomial, by studying its higher derivatives. We will also present a series of examples in the last section of the paper.
2 Proof of the main results

Our proofs rely on the following lemma, which complements Lemma 1.1. in [2]:

\textbf{Lemma 2.1.} Let \( f \in \mathbb{Z}[X] \) and suppose that \( f(m) = p^s \cdot q \) for some integers \( m, s, q \) and a prime number \( p \), with \( s \geq 2 \) and \( p \nmid qf'(m) \). If for two positive real numbers \( A \) and \( B \) we have \( A < |m| - |q| < |m| + |q| < B \), and \( f \) has no roots in the annular region \( A < |z| < B \), then \( f \) is irreducible over \( \mathbb{Q} \).

The desired results will be obtained by combining Lemma 2.1 or parts of its proof with some suitable estimates for polynomial roots.

Proof of Lemma 2.1. Let \( f(X) = \sum_{i=0}^{n} a_i X^i \) and assume that \( f \) factors as \( f(X) = f_1(X) \cdot f_2(X) \), with \( f_1, f_2 \in \mathbb{Z}[X] \), \( \deg f_1 \geq 1 \) and \( \deg f_2 \geq 1 \). Then, since \( f(m) = p^s \cdot q = f_1(m) \cdot f_2(m) \), \( f'(m) = f_1'(m)f_2(m) + f_1(m)f_2'(m) \) and \( p \nmid qf'(m) \), one of the integers \( f_1(m) \), \( f_2(m) \) must be divisible by \( p^s \), so the other must divide \( q \), say \( f_1(m) \mid q \). In particular, we have \( |f_1(m)| \leq |q| \).

Assume now that \( f \) factors as \( f(X) = a_n(X-\theta_1) \cdots (X-\theta_n) \), with \( \theta_1, \ldots, \theta_n \in \mathbb{C} \). Since \( f_1 \) is a factor of \( f \), it will factor over \( \mathbb{C} \) as \( f_1(X) = b_t(X-\theta_1) \cdots (X-\theta_t) \), say, with \( t \geq 1 \) and \( |b_t| \geq 1 \). Then one has

\[
|f_1(m)| = |b_t| \cdot \prod_{i=1}^{t} |m-\theta_i| \geq \prod_{i=1}^{t} |m-\theta_i|. \tag{1}
\]

The fact that the roots of \( f \) lie outside the annulus \( A < |z| < B \) shows that for each index \( i \in \{1, \ldots, t\} \) we either have

\[
|m-\theta_i| \geq |m| - |\theta_i| \geq |m| - A, \quad \text{if } |\theta_i| \leq A,
\]

or

\[
|m-\theta_i| \geq |\theta_i| - |m| \geq B - |m|, \quad \text{if } |\theta_i| \geq B.
\]

Since by hypothesis we have \( A < |m| - |q| < |m| + |q| < B \), we conclude that \( |m-\theta_i| > |q| \) for each \( i = 1, \ldots, t \), so by (1) we obtain \( |f_1(m)| > |q| \), which is a contradiction. This completes the proof of the lemma. □

Proof of Theorem 1.1. Note first that since \( f(b) = p^s \) and \( p \nmid f'(b) \), \( f \) must be a primitive polynomial. Let us assume that \( f \) factors as \( f(X) = f_1(X) \cdot f_2(X) \), with \( f_1, f_2 \in \mathbb{Z}[X] \), \( \deg f_1 \geq 1 \) and \( \deg f_2 \geq 1 \). Reasoning as in the proof of Lemma 2.1 with \( q = 1 \) and \( m = b \), we deduce that \( |f_1(b)| = 1 \).

We will employ now the elegant method used in [10] and [12] for the proof of Theorem B. First, we show that any complex zero \( \theta \) of \( f \) either has nonpositive real part or satisfies

\[
|\theta| < \frac{1 + \sqrt{4b-3}}{2}. \tag{2}
\]
To see this, we observe that if $|\theta| > 1$ and $\Re(\theta) > 0$ we obtain

$$
0 \geq \left| a_n + \frac{a_{n-1}}{\theta} \right| - (b - 1) \left( \frac{1}{|\theta|^2} + \cdots + \frac{1}{|\theta|^n} \right) \\
> \Re \left( a_n + \frac{a_{n-1}}{\theta} \right) - \frac{b - 1}{|\theta|^2 - |\theta|} \\
> 1 - \frac{b - 1}{|\theta|^2 - |\theta|} = \frac{|\theta|^2 - |\theta| - (b - 1)}{|\theta|^2 - |\theta|},
$$

which gives a contradiction for $|\theta| \geq (1 + \sqrt{4b - 3})/2$. Note that if $|\theta| \leq 1$, (2) holds trivially, so we may assume $|\theta| > 1$. Then we either have $\Re(\theta) \leq 0$, or $\theta$ must satisfy (2).

In the former case we have $|b - \theta| \geq b > 1$, while in the latter case we have

$$|\theta| < \frac{1 + \sqrt{4b - 3}}{2} \leq b - 1$$

if $b \geq 3$, which also yields $|b - \theta| > 1$. In view of (1) we then obtain $|f_1(b)| > 1$, a contradiction. We have therefore proved the irreducibility of $f$ for $b \geq 3$.

Let us assume now that $b = 2$. By the argument above, if $\theta$ is a root of $f$, we either have $\Re(\theta) \leq 0$, or $|\theta| < (1 + \sqrt{5})/2$. We will prove that in fact, all the roots of $f$ have real part less than $3/2$. To see this, we first observe that a root $\theta$ of $f$ with $|\arg \theta| > \pi/4$ must have $\Re(\theta) < (1 + \sqrt{5})/(2\sqrt{2}) < 3/2$, since $|\theta| < (1 + \sqrt{5})/2$. We may therefore assume that $|\arg \theta| \leq \pi/4$, and hence $\Re(1/\theta) \geq 0$ and $\Re(1/\theta^2) \geq 0$. Moreover, we have to consider only polynomials $f$ with $\deg f \geq 3$, since no polynomial of degree 2 with coefficients 0 or 1 satisfies all the hypotheses in the statement of the theorem. Let us now assume to the contrary that $\Re(\theta) \geq 3/2$. Then $|\theta| \geq 3/2$, which yields

$$
0 = \left| \frac{f(\theta)}{\theta^n} \right| \geq \left| 1 + \frac{a_{n-1}}{\theta} + \frac{a_{n-2}}{\theta^2} \right| - \left( \frac{1}{\theta^3} + \cdots + \frac{1}{\theta^n} \right) \\
> \Re \left( 1 + \frac{a_{n-1}}{\theta} + \frac{a_{n-2}}{\theta^2} \right) - \frac{1}{|\theta|^2(|\theta| - 1)} \\
\geq 1 - \frac{1}{|\theta|^2(|\theta| - 1)} = \frac{|\theta|^2 - |\theta| - 1}{|\theta|^2(|\theta| - 1)} > 0,
$$

a contradiction.

The fact that all the roots of $f$ have real part less than $3/2$ shows now that the polynomial $f_1(X + 3/2) = b_i(X + 3/2 - \theta_1) \cdots (X + 3/2 - \theta_i)$ has positive coefficients. Indeed, if $\theta_i$ is a real root of $f_1$, then the linear factor $X + 3/2 - \theta_i$ has positive coefficients, while if $\theta_i$ is not real, we pair it with its complex conjugate $\overline{\theta_i}$ and notice that

$$(X + 3/2 - \theta_i)(X + 3/2 - \overline{\theta_i}) = X^2 + 2\Re(3/2 - \theta_i)X + |3/2 - \theta_i|^2,$$
Irreducibility criteria

has too positive coefficients. Therefore \( f_1(-X + 3/2) \) has alternating coefficients, and hence for any \( X > 0 \) we have \( |f_1(-X + 3/2)| < f_1(X + 3/2) \). Letting now \( X = 1/2 \) we deduce that \( f_1(2) > |f_1(1)| \). Since 1 is not a root of \( f_1 \) and \( f_1(1) \) is an integer, we obtain \( |f_1(2)| > 1 \), which is a contradiction. This completes the proof of the theorem. \( \square \)

Proof of Theorem 1.2. Here we only need to observe that our assumption on the size of \( |a_0| \) forces the absolute values of the \( \theta_i \)'s to be greater than \(|m| + |q|\). Indeed, if \(|\theta_j| \leq |m| + |q|\) for an index \( j \in \{1, \ldots, n\} \), then since \( a_0 = -\sum_{i=1}^n a_i \theta_j \), we would obtain \(|a_0| \leq \sum_{i=1}^n |a_i| \cdot |\theta_j| \leq \sum_{i=1}^n |a_i| \cdot (|m| + |q|) \), a contradiction. The rest of the proof follows now in a manner similar to that given for Lemma 2.1. \( \square \)

Proof of Theorem 1.3. We will actually prove a more general result, that depends on a suitable set of parameters:

Lemma 2.2. Let \( f(X) = \sum_{i=0}^n a_i X^{d_i} \in \mathbb{Z}[X] \), with \( 0 = d_0 < d_1 < \cdots < d_n \) and \( a_0 a_1 \cdots a_n \neq 0 \). Suppose that \( f(m) = p^s \cdot q \) for some integers \( m, s, q \) and a prime number \( p \), with \( s \geq 2 \) and \( p \nmid q f'(m) \). Suppose also that there exist a sequence of positive real numbers \( \mu_0, \mu_1, \ldots, \mu_n \) and an index \( j \in \{0, \ldots, n\} \) such that \( \sum_{k \neq j} \mu_k \leq 1 \) and

\[
\max_{k < j} \left( \frac{1}{\mu_k} \cdot \frac{|a_k|}{|a_j|} \right)^{\frac{1}{d_k - d_j}} < |m| - |q| < |m| + |q| < \min_{k > j} \left( \mu_k \cdot \frac{|a_j|}{|a_k|} \right)^{\frac{1}{d_j - d_k}}.
\]

Then \( f \) is irreducible over \( \mathbb{Q} \).

Here we obviously have to ignore the left-most inequality if \( j = 0 \), and the right-most one if \( j = n \). Note that the inequalities in the statement of Lemma 2.2 are satisfied if

\[
|m| > |q| \quad \text{and} \quad |a_j| > \max_{k \neq j} \frac{|a_k| \cdot (|m| + |q| \cdot \text{sign}(k - j))^{d_k - d_j}}{\mu_k},
\]

so if \( f(m) = p^s \), \( s \geq 2 \) for an integer \( m \) with \(|m| \geq 2 \) and a prime number \( p \) such that \( p \nmid f'(m) \), and \( f \) has one sufficiently large coefficient, then it must be irreducible over \( \mathbb{Q} \).

By choosing in Lemma 2.2 different sequences of positive real numbers \( \mu_0, \mu_1, \ldots, \mu_n \) that satisfy \( \sum_{k \neq j} \mu_k \leq 1 \), we may obtain various irreducibility conditions. For instance, we may simply choose \( \mu_k = 1/n \) for \( k \neq j \), or \( \mu_k = 2^{-n \binom{n}{k}} \) for \( k \neq j \). For an example when the \( \mu_k \)'s depend on the coefficients of \( f \), we take \( \mu_k = |a_k|/\sum_{i \neq j} |a_i| \) for \( k \neq j \), and obtain Theorem 1.3.

We also note that a direct use of the triangle inequality as in Theorems 1.2 and 1.4 gives sharper conditions than those exhibited by Lemma 2.2 in the cases \( j = 0 \) and \( j = n \).
Proof of Lemma 2.2. Assume that $f$ factors as $f(X) = a_n(X - \theta_1) \ldots (X - \theta_m)$, with $\theta_1, \ldots, \theta_m \in \mathbb{C}$, let

$$A = \max_{k<j} \left( \frac{1}{\mu_k} \cdot \frac{|a_k|}{|a_j|} \right)^{\frac{1}{d_k - d_j}}$$

and $B = \min_{k>j} \left( \mu_k \cdot \frac{|a_j|}{|a_k|} \right)^{\frac{1}{d_k - d_j}}$, 

and note that according to our hypotheses $A$ must be strictly smaller than $B$.

M. Fujiwara proved in [7] the following flexible result on the location of the roots of a complex polynomial:

Let $P(z) = \sum_{i=0}^n a_i z^{d_i} \in \mathbb{C}[z]$, with $0 = d_0 < d_1 < \cdots < d_n$ and $a_0 a_1 \ldots a_n \neq 0$. Let also $a_0, \ldots, a_{n-1} \in (0, \infty)$ such that $\frac{1}{\mu_0} + \cdots + \frac{1}{\mu_{n-1}} \leq 1$. Then all the roots of $P$ are contained in the disk $|z| \leq R$, where

$$R = \max_{0 \leq j \leq n-1} \left( \mu_j \frac{|a_j|}{|a_n|} \right)^{\frac{1}{d_n - d_j}}.$$

We will adapt here the classical method of Fujiwara to find information on the location of the roots of $f$. More precisely, we will prove that $f$ has no roots in the annular region $A < |z| < B$, as required in Lemma 2.1. To see this, let us assume that $A < |\theta_i| < B$ for some index $i \in \{1, \ldots, d_n\}$. Then from $A < |\theta_i|$ we deduce that $\mu_k |a_j| \cdot |\theta_i|^{d_j} > |a_k| \cdot |\theta_i|^{d_k}$ for each $k < j$, while from $|\theta_i| < B$ we find that $\mu_k |a_j| \cdot |\theta_i|^{d_j} > |a_k| \cdot |\theta_i|^{d_k}$ for each $k > j$. Adding term by term these inequalities and using the fact that $\sum_{k \neq j} \mu_k \leq 1$, we obtain

$$|a_j| \cdot |\theta_i|^{d_j} > \sum_{k \neq j} |a_k| \cdot |\theta_i|^{d_k}. \quad (3)$$

On the other hand, since $f(\theta_i) = 0$ we must have

$$0 \geq |a_j| \cdot |\theta_i|^{d_j} - |a_k| \cdot \theta_i^{d_k} \geq |a_j| \cdot |\theta_i|^{d_j} - \sum_{k \neq j} |a_k| \cdot |\theta_i|^{d_k},$$

which contradicts (3). The conclusion follows now by Lemma 2.1. \( \square \)

Proof of Theorem 1.4. In this case our assumption on the size of $|a_n|$ forces all the $\theta_i$’s to have absolute value smaller than $|m| - |q|$, for otherwise, if $|\theta_j| \geq |m| - |q|$ for an index $j \in \{1, \ldots, n\}$, we would have

$$0 = \sum_{i=0}^n a_i \theta_i^{i-n} \geq |a_n| - \sum_{i=0}^{n-1} |a_i| \cdot |\theta_j|^{i-n} \geq |a_n| - \sum_{i=0}^{n-1} |a_i| \cdot (|m| - |q|)^{i-n},$$

a contradiction. \( \square \)

Proof of Corollary 1.6. Here we use the fact that $1 > \sum_{i=0}^{n-1} (|m| - |q|)^{i-n}$ for $|q| = 1$ and $|m| \geq 3$. Notice that in the statement of Corollary 1.6 one may consider integer polynomials with coefficients of modulus at most 1 instead of Littlewood polynomials. \( \square \)
Proof of Proposition 1.7. In order to find information on the location of the roots of \( f \), we use now a classical result of Cowling and Thron (see [5], [6]):

Let \( P(z) = a_0 z^{d_0} + a_1 z^{d_1} + \cdots + a_n z^{d_n} \in \mathbb{C}[z] \) with all \( a_j \neq 0 \), \( 0 = d_0 < d_1 < \cdots < d_n \), and \( m_j = (d_j - d_{j-1})^{-1} \), \( j = 1, 2, \ldots, n \). Let \( \mu_0 = 0 \), \( \mu_n = 1 \) and \( \mu_1, \ldots, \mu_{n-1} \) be arbitrary positive constants. Then all the zeros of \( P \) lie in the disc

\[
|z| \leq A = \max_{1 \leq j \leq n} \left\{ \frac{(1 + \mu_{j-1})}{\mu_j} \cdot \frac{|a_{j-1}|}{|a_j|} \right\}^{m_j}.
\]

Indeed, if \( P \) would have one root \( z_0 \) with \( |z_0| > A \), then we would obtain

\[
\begin{align*}
\mu_1|a_1| \cdot |z_0|^{d_1} &> (1 + \mu_0)|a_0| \cdot |z_0|^{d_0} \\
\mu_2|a_2| \cdot |z_0|^{d_2} &> (1 + \mu_1)|a_1| \cdot |z_0|^{d_1} \\
\mu_3|a_3| \cdot |z_0|^{d_3} &> (1 + \mu_2)|a_2| \cdot |z_0|^{d_2} \\
& \vdots \\
\mu_n|a_n| \cdot |z_0|^{d_n} &> (1 + \mu_{n-1})|a_{n-1}| \cdot |z_0|^{d_{n-1}},
\end{align*}
\]

which after summation and cancellation of equal terms on each side would imply that

\[
|a_n| \cdot |z_0|^{d_n} > \sum_{i=0}^{n-1} |a_i| \cdot |z_0|^{d_i}.
\]

On the other hand, since \( P(z_0) = 0 \), we must have

\[
|a_n| \cdot |z_0|^{d_n} \leq \sum_{i=0}^{n-1} |a_i| \cdot |z_0|^{d_i},
\]

which is a contradiction.

This result shows that the roots of our polynomial \( f \) satisfy \( |\theta_i| \leq A \) for \( i = 1, \ldots, d_n \), and the conclusion follows by Lemma 2.1. \( \square \)

Proof of Proposition 1.8. We will prove here that the roots of \( f \) satisfy

\[
|\theta_i| \geq B = \min_{1 \leq j \leq n} \left\{ \frac{\mu_{j-1}|a_{j-1}|}{(1 + \mu_j)|a_j|} \right\}^{m_j} 
\]

uniformly for \( i = 1, \ldots, d_n \). To see this, let us assume that \( |\theta_i| < B \) for some index \( i \). Then we obtain successively

\[
(1 + \mu_1)|a_1| \cdot |\theta_1|^{d_1} < \mu_0|a_0| \cdot |\theta_0|^{d_0} \\
(1 + \mu_2)|a_2| \cdot |\theta_1|^{d_2} < \mu_1|a_1| \cdot |\theta_1|^{d_1} \\
(1 + \mu_3)|a_3| \cdot |\theta_2|^{d_3} < \mu_2|a_2| \cdot |\theta_2|^{d_2} \\
& \vdots \\
(1 + \mu_n)|a_n| \cdot |\theta_{n-1}|^{d_n} < \mu_{n-1}|a_{n-1}| \cdot |\theta_{n-1}|^{d_{n-1}}.
\]

Recalling that \( \mu_0 = 1 \) and \( \mu_n = 0 \), adding term by term these inequalities and canceling the equal terms on both sides, we find that

\[
|a_0| \cdot |\theta_0|^{d_0} > \sum_{j=1}^{n} |a_j| \cdot |\theta_j|^{d_j}.
\]

On the other hand, since \( f(\theta_i) = 0 \) we must have

\[
|a_0| \cdot |\theta_0|^{d_0} \leq \sum_{j=1}^{n} |a_j| \cdot |\theta_j|^{d_j},
\]

which is a contradiction.

Let us assume now as in the proof of Lemma 2.1 that \( f \) decomposes as \( f = f_1 f_2 \), with \( \deg f_1 \geq 1 \) and \( \deg f_2 \geq 1 \). Then we obtain \( |f_1(m)| \leq |q| \), while the
roots of $f_1$ satisfy
\[ |m - \theta_i| \geq |\theta_i| - |m| \geq B - |m| > |q|, \quad i = 1, \ldots, t, \]
which by (1) gives the contradiction $|f_1(m)| > |q|$ and completes the proof. \(\square\)

**Proof of Proposition 1.9.** For the proof we use the following classical result given in [11]:

If $\mu = (\mu_1, \mu_2, \ldots, \mu_n)$ is an arbitrary set of positive numbers, then all the characteristic roots of the $n \times n$ complex matrix $M = (a_{ij})$ lie in the disk $|z| \leq A_\mu$ where
\[ A_\mu = \max_{1 \leq i \leq n} \sum_{j=1}^{n} \frac{\mu_j}{\mu_i} |a_{ij}|. \] (4)

Indeed, for any characteristic root $\lambda$ of $M$ the system of equations
\[ \sum_{j=1}^{n} a_{ij} x_j = \lambda x_i, \quad i = 1, 2, \ldots, n \] (5)
has a non-trivial solution $(x_1, x_2, \ldots, x_n)$. Let us set $x_j = \mu_j y_j$ and denote by $y_m$ the $y_j$ of maximum modulus. By the $m$th equation of (5) we then infer that
\[ |\lambda \mu_m y_m| \leq \sum_{j=1}^{n} |a_{mj}| \mu_j |y_j| \leq \left( \sum_{j=1}^{n} |a_{mj}| \mu_j \right) |y_m|. \]
Hence, $|\lambda| \leq A_\mu$.

If we apply this result to the companion matrix of the polynomial $\tilde{f}(X) = \frac{1}{a_n} f(X)$:
\[
M_f = \begin{bmatrix}
0 & 1 & 0 & \cdots & 0 & 0 \\
0 & 0 & 1 & \cdots & 0 & 0 \\
\vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\
0 & 0 & 0 & \cdots & 0 & 1 \\
-\frac{a_n}{a_1} & -\frac{a_1}{a_2} & -\frac{a_2}{a_3} & \cdots & -\frac{a_{n-2}}{a_n} & -\frac{a_{n-1}}{a_n}
\end{bmatrix},
\]
we find that all the roots of $f$ lie in the disk
\[ |z| \leq A = \max \left\{ \frac{\mu_2}{\mu_1}, \frac{\mu_3}{\mu_2}, \ldots, \frac{\mu_n}{\mu_{n-1}}, \sum_{j=1}^{n} \frac{\mu_j}{\mu_n} \cdot \frac{|a_{j-1}|}{|a_n|} \right\}, \]
so the roots of $f_1$ satisfy
\[ |m - \theta_i| \geq |m| - |\theta_i| \geq |m| - A > |q|, \quad i = 1, \ldots, t, \]
which by (1) gives the contradiction and completes the proof. \(\square\)
Proof of Proposition 1.10. For the proof we use in this case a classical result of Ballieu (see [1], [9]) on the location of the roots of a complex polynomial:

Let \( P(z) = a_0 + a_1 z + \cdots + a_n z^n \in \mathbb{C}[z] \) with \( a_0 a_n \neq 0 \) and let \( \mu_0 = 0 \) and \( \mu_1, \ldots, \mu_n \) be arbitrary positive constants. Then all the roots of \( P \) lie in the disc

\[
|z| \leq A = \max_{0 \leq j \leq n-1} \left\{ \frac{\mu_j}{\mu_{j+1}} + \frac{\mu_n}{\mu_{j+1}} \cdot \left| \frac{a_j}{a_n} \right| \right\}.
\]

This result follows immediately by using (4) for the transposed of \( \mathcal{M}_f \).

Using again the same notations as in the proof of Lemma 2.1, we have \( |f_1(m)| \leq |q| \), while the roots of \( f_1 \) satisfy

\[
|m - \theta_i| \geq |m| - |\theta_i| \geq |m| - A > |q|, \quad i = 1, \ldots, t,
\]

which by (1) gives the desired contradiction. \( \Box \)

The last result we will prove is the following variant of Lemma 2.1, which allows one to consider higher derivatives in the study of the total number of irreducible factors of a given polynomial. Here for a polynomial \( f \in \mathbb{Z}[X] \) the notation \( \Omega(f) \leq n \) means that \( f \) is a product of at most \( n \) irreducible factors over \( \mathbb{Q} \), counting multiplicities.

Lemma 2.3. Let \( f \in \mathbb{Z}[X] \) and suppose that \( f(m) = p^s \cdot q \) for some integers \( m, s, q \) and a prime number \( p \), with \( s \geq 1 \) and \( p \nmid q \). Suppose also that \( p^t \nmid f^{(i)}(m) \) for some \( i \geq 1 \). If for two positive real numbers \( A \) and \( B \) we have \( A < |m| - |q| < |m| + |q| < B \), and \( f \) has no roots in the annular region \( A < |z| < B \), then \( \Omega(f) \leq \min(i, s) \).

Proof: We will first prove that for each factor \( f_1 \) of \( f \) we must have \( |f_1(m)| > q \). To see this, let us assume that \( f \) factors as \( f(X) = a_n (X - \theta_1) \cdots (X - \theta_n) \), with \( \theta_1, \ldots, \theta_n \in \mathbb{C} \). This implies that \( f_1 \), as a factor of \( f \), must factor over \( \mathbb{C} \) as \( f_1(X) = \beta_1 (X - \theta_1) \cdots (X - \theta_t) \), say, with \( t \geq 1 \) and \( |\beta_t| \geq 1 \). Then, like in the proof of Lemma 2.1 one has

\[
|f_1(m)| = |\beta_t| \cdot \prod_{i=1}^{t} |m - \theta_i| \geq \prod_{i=1}^{t} |m - \theta_i|.
\]  

(6)

The fact that the roots of \( f \) lie outside the annulus \( A < |z| < B \) shows that for each index \( i \in \{1, \ldots, t\} \) we either have

\[
|m - \theta_i| \geq |m| - |\theta_i| \geq |m| - A, \quad \text{if} \quad |\theta_i| \leq A,
\]

or

\[
|m - \theta_i| \geq |\theta_i| - |m| \geq B - |m|, \quad \text{if} \quad |\theta_i| \geq B.
\]

Since by hypothesis we have \( A < |m| - |q| < |m| + |q| < B \), we conclude that \( |m - \theta_i| > |q| \) for each \( i = 1, \ldots, t \), so by (6) we obtain \( |f_1(m)| > |q| \), as desired. Moreover, this shows that in fact \( f_1(m) \) must be divisible by \( p \), so \( \Omega(f) \leq s \).
We will use now the condition on the $i$th derivative of $f$ to prove that $f$ cannot be written as a product of more than $i$ irreducible factors. Assume by contrary that $f$ decomposes as $f = f_1 \cdots f_k$ with $f_1, \ldots, f_k$ irreducible over $\mathbb{Q}$ and $k > i$, and notice that in the expansion of $f^{(i)}$ the terms $f_1^{(i_1)} \cdots f_k^{(i_k)}$ may be indexed by partitions of $i$: $i_1 + \cdots + i_k = i$, $i_1 \geq 0, \ldots, i_k \geq 0$. Since $k > i$, each term in this expansion must contain at least one factor $f_l^{(i_l)}$ with $i_l = 0$, so by the argument above, each term $f_1^{(i_1)}(m) \cdots f_k^{(i_k)}(m)$ must be divisible by $p$, which contradicts our hypothesis that $p \nmid f^{(i)}(m)$ and completes the proof of the lemma.

Using Lemma 2.3, one may easily rephrase the irreducibility criteria stated so far, to derive bounds for the total number of irreducible factors for polynomials that take a value divisible by a prime power. We end by noting that one may also easily formulate separability criteria, by applying the irreducibility conditions in the results above to the derivative of a given polynomial.

3 Examples.

i) Let $f(X) = X^7 + 4X^6 + 3X^5 + 4X^4 + 8X^3 + 9X^2 + 7$ and note that $f$ is obtained by replacing the powers of 10 with the powers of $X$ in the decimal representation of $3^{15}$. Since $3 \nmid f'(10) = 9568580$, $f$ is irreducible by Theorem 1.1.

ii) Let $f(X) = p^q a_1 X + a_2 X^2 + \ldots + a_n X^n \in \mathbb{Z}[X]$, with $p$ a prime number, $q$ a nonzero integer, $s \geq 2$, $a_s \neq 0$ and $p \nmid qa_1$. If $p^s > \sum_{i=1}^{n} |a_i| \cdot |q|^{i-1}$, then $f$ must be irreducible over $\mathbb{Q}$. This follows immediately by taking $m = 0$ in Theorem 1.2. One such polynomial is for instance $f(X) = 250 + 2X + 3X^2 - 3X^3 + 5X^4 + 4X^5$. Here we have $p = 5$, $s = 3$, $q = 2$ and $125 > \sum_{i=1}^{5} |a_i| 2^{i-1} = 124$, so $f$ is an irreducible polynomial.

iii) Let $f(X) = 1 - 2X - X^2 + X^3 + 424X^4 - X^5 - X^6 - X^7$ and note that $f(2) = 3^8$, a prime power. Here $m = 2$, $q = 1$, $f'(2) = 12854$ is not divisible by 3, and we may take $j = 4$ in Theorem 1.3, since $424 = |a_4| > (|m| + |q|)^{d_4 - d_4} \cdot \sum_{i \neq 4} |a_i| = 3^3 \cdot 8 = 216$. We therefore conclude that $f$ is an irreducible polynomial.

iv) Let us take $f(X) = 3967 - 401X^2 - 251X^2 - 171X^3 - 14X^4 - 5X^5$. Here $\sum_{i=0}^{5} a_i = 3125 = 5^5$, $|a_0| > \sum_{i=1}^{5} |a_i| 2^i$ and $\sum_{i=1}^{5} ia_i = -1497$, which is not divisible by 5, so $f$ is irreducible by Corollary 1.5.

v) Let $f(X) = -1 + X - X^2 - X^3 - X^4 + X^5$. Here we have $f(3) = 27$ and $2 \nmid f'(3) = 265$, so $f$ is irreducible by Corollary 1.6.

vi) If we take $\mu_j = 1$ for $j = 1, \ldots, n$, in Proposition 1.7, we see that a polynomial $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ with $a_0a_1 \ldots a_n \neq 0$, $|a_0| < |a_1|$ and $2|a_{j-1} < |a_j|$ for $j = 2, 3, \ldots, n$ is irreducible over $\mathbb{Q}$ if $f(m)$ is a prime power $p^s$, $s \geq 2$ for an integer $m$ with $|m| \geq 2$ and $p \nmid f'(m)$. One such polynomial is for instance $f(X) = 1 - 2X - 5X^2 + 11X^3 + 24X^4 + 61X^5$, since $f(2) = 2401 = 7^4$, and $7 \nmid f'(2) = 5758$. 


vii) From Proposition 1.9 with $\mu_1 = \mu_2 = \ldots = \mu_n = 1$ it follows that a polynomial $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ with $a_0 a_n \neq 0$, $|a_n| < |a_0| + |a_1| + \cdots + |a_{n-1}|$ and such that $f(m) = p^q$ for integers $m, p, s, q$ with $p$ a prime number, $s \geq 2$, $|m| > |q| + (|a_0| + |a_1| + \cdots + |a_{n-1}|)/|a_n|$, and $p \nmid qf'(m)$ must be irreducible over $\mathbb{Q}$. For such an example, take for instance $f(X) = -7 - 7X + 6X^2 + 9X^3 + 3X^4 + 8X^5$ and $m = 10$. Here $f(10) = 839523 = 3 \cdot 23^4$, so if we let $p = 23$ and $q = 3$ we see that $p \nmid qf'(10) = 3^2 \cdot 7 \cdot 19753$, hence $f$ must be irreducible.

viii) For an example related to Corollary 1.11, let us consider now the polynomial $f(X) = 6 - 5X + 5X^2 + X^3 + 9X^4 + 2X^5 + 6X^6$. Here $f(10) = 6291456 = 2^{21} \cdot 3$ and $f'(10) = 3736395$, so we may take $m = 10, p = 2$ and $q = 3$. Since $p \nmid qf'(m)$, and $|m| - |q| = 7 > \max_{0 \leq i \leq 5} (1 + |a_i|/|a_0|) = 5/2$, $f$ is an irreducible polynomial.

Acknowledgements This work was partially supported by CNCSIS-UEFISCSU, project PNII-IDEI 51, code 304/2007.

References


A.I. Bonciocat, N.C. Bonciocat, and A. Zaharescu


Received: 04.09.2010
Accepted: 10.10.2010.