Canad. Math. Bull. Vol. **52** (4), 2009 pp. 511–520

The Irreducibility of Polynomials That Have One Large Coefficient and Take a Prime Value

Anca Iuliana Bonciocat and Nicolae Ciprian Bonciocat

Abstract. We use some classical estimates for polynomial roots to provide several irreducibility criteria for polynomials with integer coefficients that have one sufficiently large coefficient and take a prime value.

1 Introduction

Many classical irreducibility criteria for polynomials with integer coefficients rely on the existence of a suitable prime divisor in the canonical decomposition of some of their coefficients. Other irreducibility criteria rely on the existence of a suitable prime divisor of the value that a given polynomial takes at a specified integral argument. For instance, in [13] Pólya and Szegö give the following nice result of A. Cohn:

Theorem **(A)** *If a prime p is expressed in the decimal system as*

$$p=\sum_{i=0}^{n} a_i 10^i, \quad 0 \le a_i \le 9,$$

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 [3]:

Theorem **(B)** *If a prime p is expressed in the number system with base $b \ge 2$ as*

$$p=\sum_{i=0}^{n} a_i b^i, \quad 0 \le a_i \le b-1,$$

then the polynomial $\sum_{i=0}^{n} a_i X^i$ is irreducible in $\mathbb{Z}[X]$.

Received by the editors June 8, 2006; revised July 4, 2006.
This work was partially supported by the CEEX Programme of the Romanian Ministry of Education and Research, contract CEx05-D11-11/2005.
AMS subject classification: Primary: 11C08; secondary: 11R09.
Keywords: Estimates for polynomial roots, irreducible polynomials.

https://doi.org/10.4153/CMB-2009-052-9 Published online by Cambridge University Press

Elementary proofs of these results have been obtained by M. Ram Murty in [14] where an analogue of Theorem B for polynomials with coefficients in $\mathbb{F}_q[t]$ with $\mathbb{F}_q$ a finite field was also established. Some classes of composite numbers enjoy this nice property too. In this respect, Filaseta [6] obtained another generalization of Theorem B by replacing the prime p by a composite number wp with $w < b$:

***Theorem* (C)** *Let p be a prime number, w and b positive integers, $b \geq 2$, $w < b$, and suppose that wp is expressed in the number system with base b as*

$$wp = \sum_{i=0}^{n} a_i b^i, \quad 0 \leq a_i \leq b-1.$$

Then the polynomial $\sum_{i=0}^{n} a_i X^i$ is irreducible over the rationals.

Cohn's Theorem was also generalized in [3] and [7] by permitting the coefficients of f to be different from digits. For instance, the following irreducibility criterion for polynomials with non-negative coefficients was proved in [7].

***Theorem* (D)** *Let $f(X) = \sum_{i=0}^{n} a_i X^i$ be such that $f(10)$ is a prime. If the a_i's satisfy $0 \leq a_i \leq a_n 10^{30}$ for each $i = 0, 1, \dots, n-1$, then $f(X)$ is irreducible.*

Similar irreducibility conditions for multivariate polynomials over an arbitrary field have been obtained in [2].

In this paper we will establish some irreducibility conditions for polynomials with integer coefficients that have one large coefficient and take a prime value, by using several estimates on the location of their roots. The results we will prove rely on the following lemma:

Lemma 1.1 *Let f be a polynomial with integer coefficients and suppose that for an integer m, a prime number p, and a nonzero integer q we have $f(m) = p \cdot q$. 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 $\mathbb{Q}$.*

Our irreducibility conditions will be obtained by combining Lemma 1.1 with some classical estimates for polynomial roots. The first irreducibility criterion that we will prove is given by the following

Theorem 1.2 *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 for an integer m, a prime number p, and a nonzero integer q we have $f(m) = p \cdot q$. Suppose also that there exist a sequence of positive real numbers $\mu_0, \mu_1, \dots, \mu_n$ and an index $j \in \{0, \dots, n\}$ such that $\sum_{k \neq j} \mu_k \leq 1$ and*

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

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

https://doi.org/10.4153/CMB-2009-052-9 Published online by Cambridge University Press

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 Theorem 1.2 are satisfied if

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

so if $f(m)$ is a prime number for an integer m with $|m| \geq 2$, and f has one sufficiently large coefficient, then it must be irreducible over $\mathbb{Q}$.

One may obtain various irreducibility conditions by choosing different sequences of positive real numbers $\mu_0, \mu_1, \ldots, \mu_n$ satisfying $\sum_{k\neq j} \mu_k \leq 1$. For instance, one 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 μ_k's depend on the coefficients of f, take $\mu_k = |a_k|/\sum_{i\neq j} |a_i|$ for $k \neq j$. Then we obtain the following.

Corollary 1.3 *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 for an integer m, a prime number p, and a nonzero integer q with $|m| > |q|$ we have $f(m) = p \cdot q$. If for an index $j \in \{1, \ldots, n-1\}$ we have*

$$|a_j| > (|m| + |q|)^{d_n - d_j} \cdot \sum_{i\neq j} |a_i|,$$

then f is irreducible over $\mathbb{Q}$.

For the remaining cases $j = 0$ and $j = n$ we obtain sharper conditions by a direct use of the triangle inequality. These conditions are given by the following two results.

Proposition 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 for an integer m, a prime number p, and a nonzero integer q we have $f(m) = p \cdot q$ and*

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

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

Proposition 1.5 *Let $f(X) = \sum_{i=0}^n a_i X^i \in \mathbb{Z}[X]$, $a_0 a_n \neq 0$. Suppose that for a prime number p, and two nonzero integers m and q with $|m| > |q|$ we have $f(m) = p \cdot q$ and*

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

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

In particular, from Propositions 1.4 and 1.5 one obtains the following irreducibility conditions respectively.

Corollary 1.6 *If we write a prime number as a sum of integers $a_0, \ldots, a_n$, with $a_0 a_n \neq 0$ 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 $\mathbb{Q}$.*

https://doi.org/10.4153/CMB-2009-052-9 Published online by Cambridge University Press

Corollary 1.7 *If all the coefficients of a polynomial f are ± 1, and $f(m)$ is a prime number for an integer m with $|m| \geq 3$, then f is irreducible over $\mathbb{Q}$.*

We will also prove the following related results.

Theorem 1.8 *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 for an integer m, a prime number p, and a nonzero integer q we have $f(m) = p \cdot q$ and let $\mu_0 = 0$, $\mu_n = 1$ and $\mu_1, \ldots, \mu_{n-1}$ be arbitrary positive constants. If*

$$|m| - |q| > \max_{1 \leq j \leq n} \left\{ \frac{(1 + \mu_{j-1})|a_{j-1}|}{\mu_j |a_j|} \right\}^{\frac{1}{d_j - d_{j-1}}},$$

then f is irreducible over $\mathbb{Q}$.

Theorem 1.9 *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 for an integer m, a prime number p, and a nonzero integer q we have $f(m) = p \cdot q$ and let $\mu_0 = 1$, $\mu_n = 0$ and $\mu_1, \ldots, \mu_{n-1}$ be arbitrary positive constants. If*

$$|m| + |q| < \min_{1 \leq j \leq n} \left\{ \frac{\mu_{j-1}|a_{j-1}|}{(1 + \mu_j)|a_j|} \right\}^{\frac{1}{d_j - d_{j-1}}},$$

then f is irreducible over $\mathbb{Q}$.

Theorem 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 for an integer m, a prime number p, and a nonzero integer q we have $f(m) = p \cdot q$ and let $\mu_1, \ldots, \mu_n$ be arbitrary positive constants. If*

$$|m| - |q| > \max\left\{ \frac{\mu_2}{\mu_1}, \frac{\mu_3}{\mu_2}, \ldots, \frac{\mu_n}{\mu_{n-1}}, \sum_{j=1}^{n} \frac{\mu_j}{\mu_n} \cdot \frac{|a_{j-1}|}{|a_n|} \right\},$$

then f is irreducible over $\mathbb{Q}$.

Theorem 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 for an integer m, a prime number p, and a nonzero integer q we have $f(m) = p \cdot q$. Let $\mu_0 = 0$ and $\mu_1, \ldots, \mu_n$ be arbitrary positive constants. If*

$$|m| - |q| > \max_{0 \leq j \leq n-1} \left\{ \frac{\mu_j}{\mu_{j+1}} + \frac{\mu_n}{\mu_{j+1}} \cdot \frac{|a_j|}{|a_n|} \right\},$$

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 1.12 *Let $f(X) = \sum_{i=0}^{n} a_i X^{i} \in \mathbb{Z}[X]$, with $a_0 a_n \neq 0$. Suppose that for an integer m, a prime number p, and a nonzero integer q we have $f(m) = p \cdot q$. 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 $\mathbb{Q}$.

https://doi.org/10.4153/CMB-2009-052-9 Published online by Cambridge University Press

Our results are quite flexible and may be useful in various applications when most of the classical irreducibility criteria fail. The proofs of the main results are presented in Section 2 below. In order to keep this paper self-contained, we will also include the proofs of the estimates for polynomials roots needed in our results. We will also give a series of examples in the last section of the paper.

2 Proofs of the Main Results

Proof of Lemma 1.1 Let $f(X) = \sum_{i=0}^{n} a_i X^i$ and assume that f decomposes 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 $f(m) = p \cdot q = f_1(m) \cdot f_2(m)$ and p is a prime number, one of the integers $f_1(m)$, $f_2(m)$ must divide q, say $f_1(m) \mid q$. In particular, we have $|f_1(m)| \leq |q|$. Assume now that f factorizes as $f(X) = a_n(X - \theta_1) \dots (X - \theta_n)$, with $\theta_1, \dots, \theta_n \in \mathbb{C}$. Since f_1 is a factor of f, it will factorize 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 $i \in \{1, \dots, t\}$ 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 $i = 1, \dots, t$, so by (1) we obtain $|f_1(m)| > |q|$, which is a contradiction. This completes the proof of the lemma. ∎

Proof of Theorem 1.2 Assume that f factorizes as $f(X) = a_n(X - \theta_1) \cdots (X - \theta_{d_n})$, with $\theta_1, \dots, \theta_{d_n} \in \mathbb{C}$, let

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

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

M. Fujiwara proved the following elegant and flexible result on the location of the roots of a complex polynomial in [8]:

> 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 $a_0 a_1 \dots a_n \neq 0$. Let also $\mu_0, \dots, \mu_{n-1} \in (0, \infty)$ 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
>
> $$R = \max_{0 \leq j \leq n-1} \left(\mu_j \frac{|a_j|}{|a_n|} \right)^{\frac{1}{d_n - d_j}}.$$

https://doi.org/10.4153/CMB-2009-052-9 Published online by Cambridge University Press

We will adapt Fujiwara's classical method here 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 1.1. To see this, let us assume that $A < |\theta_i| < B$ for some index $i \in \{1, \dots, d_n\}$. 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 these inequalities term by term and using the fact that $\sum_{k \neq j} \mu_k \leq 1$, we obtain

$$|a_j| \cdot |\theta_i|^{d_j} > \sum_{k \neq j} |a_k| \cdot |\theta_i|^{d_k}. \tag{2}$$

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

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

which contradicts (2). The conclusion follows now by Lemma 1.1. ∎

Proof of Proposition 1.4 Here we only need to observe that our assumption on the size of $|a_0|$ forces the absolute values of the θ_i's to be greater than $|m| + |q|$. Indeed, if $|\theta_j| \leq |m| + |q|$ for an index $j \in \{1, \dots, n\}$, then since $a_0 = -\sum_{i=1}^n a_i \cdot \theta_j^i$, we would obtain $|a_0| \leq \sum_{i=1}^n |a_i| \cdot |\theta_j|^i \leq \sum_{i=1}^n |a_i| \cdot (|m| + |q|)^i$, which is a contradiction. The rest of the proof follows now in a manner similar to that given for Lemma 1.1. ∎

Proof of Proposition 1.5 In this case our assumption on the size of $|a_n|$ forces all the the θ_i's to have absolute value smaller than $|m| - |q|$, for otherwise, if $|\theta_j| \geq |m| - |q|$ for an index $j \in \{1, \dots, n\}$, we would have

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

a contradiction. ∎

Proof of Theorem 1.8 In order to find information on the location of the roots of f, we use now a classical result of Cowling and Thron (see [4, 5]):

> 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 $m_j = (d_j - d_{j-1})^{-1}$, $j = 1, 2, \dots, n$. Let $\mu_0 = 0$, $\mu_n = 1$ and $\mu_1, \dots, \mu_{n-1}$ be arbitrary positive constants. Then all the zeros of P lie in the disc
>
> $$|z| \leq A = \max_{1 \leq j \leq n} \Big\{ \frac{(1 + \mu_{j-1})}{\mu_j} \cdot \frac{|a_{j-1}|}{|a_j|} \Big\}^{m_j}.$$

https://doi.org/10.4153/CMB-2009-052-9 Published online by Cambridge University Press

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

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

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 $|a_n|\cdot|z_0|^{d_n} \le \sum_{i=0}^{n-1}|a_i|\cdot|z_0|^{d_i}$, which is a contradiction. We note here that the estimate in the case when $\mu_1 = \mu_2 = \cdots = \mu_n = 1$ was established earlier by Kojima (see [9, 10]).

This result shows that the roots of our polynomial f satisfy $|\theta_i| \le A$ for $i = 1,\dots,d_n$, and the conclusion follows by Lemma 1.1. ∎

Proof of Theorem 1.9 We will prove here that the roots of f satisfy

$$|\theta_i| \ge B = \min_{1\le j\le n}\left\{\frac{\mu_{j-1}|a_{j-1}|}{(1+\mu_j)|a_j|}\right\}^{\frac{1}{d_j-d_{j-1}}}$$

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

$$\begin{aligned}
(1+\mu_1)|a_1|\cdot|\theta_i|^{d_1} &< \mu_0|a_0|\cdot|\theta_i|^{d_0}\\
(1+\mu_2)|a_2|\cdot|\theta_i|^{d_2} &< \mu_1|a_1|\cdot|\theta_i|^{d_1}\\
(1+\mu_3)|a_3|\cdot|\theta_i|^{d_3} &< \mu_2|a_2|\cdot|\theta_i|^{d_2}\\
&\vdots\\
(1+\mu_n)|a_n|\cdot|\theta_i|^{d_n} &< \mu_{n-1}|a_{n-1}|\cdot|\theta_i|^{d_{n-1}}.
\end{aligned}$$

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 $|a_0|\cdot|\theta_i|^{d_0} > \sum_{j=1}^{n}|a_j|\cdot|\theta_i|^{d_j}$. On the other hand, since $f(\theta_i) = 0$ we must have $|a_0|\cdot|\theta_i|^{d_0} \le \sum_{j=1}^{n}|a_j|\cdot|\theta_i|^{d_j}$, which is a contradiction.

Let us assume now as in the proof of Lemma 1.1 that f decomposes as $f = f_1f_2$, with $\deg f_1 \ge 1$ and $\deg f_2 \ge 1$. Then we obtain $|f_1(m)| \le |q|$, while the roots of f_1 satisfy

$$|m-\theta_i| \ge |\theta_i| - |m| \ge B - |m| > |q|, \quad i = 1,\dots,t,$$

which by (1) gives the contradiction $|f_1(m)| > |q|$ and completes the proof. ∎

https://doi.org/10.4153/CMB-2009-052-9 Published online by Cambridge University Press

Proof of Theorem 1.10 For the proof we use the following classical result given in [12]:

> If $\mu = (\mu_1, \mu_2, \dots, \mu_n)$ is an arbitrary set of positive numbers, then all the characteristic roots of the $n \times n$ complex matrix $\mathcal{M} = (a_{ij})$ lie on the disk $|z| \le A_\mu$ where

$$A_\mu = \max_{1 \le i \le n} \sum_{j=1}^{n} \frac{\mu_j}{\mu_i} |a_{ij}|. \tag{3}$$

Indeed, for any characteristic root λ of $\mathcal{M}$ the system of equations

$$\sum_{j=1}^{n} a_{ij} x_j = \lambda x_i, \qquad i = 1, 2, \dots, n \tag{4}$$

has a non-trivial solution $(x_1, x_2, \dots, x_n)$. Let us set $x_j = \mu_j y_j$ and denote by y_m the y_j of maximum modulus. By the mth equation of (4) we then infer that

$$|\lambda \mu_m y_m| \le \sum_{j=1}^{n} |a_{mj}| \mu_j |y_j| \le \Big(\sum_{j=1}^{n} |a_{mj}| \mu_j \Big) |y_m|.$$

Hence, $|\lambda| \le A_\mu$.

If we apply this result to the companion matrix of the polynomial $\bar{f}(X) = \frac{1}{a_n} f(X)$:

$$\mathcal{M}_{\bar{f}} = \begin{bmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \cdot & \cdot & \cdot & \cdots & \cdot & \cdot \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ -\frac{a_0}{a_n} & -\frac{a_1}{a_n} & -\frac{a_2}{a_n} & \cdots & -\frac{a_{n-2}}{a_n} & -\frac{a_{n-1}}{a_n} \end{bmatrix},$$

we find that all the roots of f lie on the disk

$$|z| \le A = \max\Big\{ \frac{\mu_2}{\mu_1}, \frac{\mu_3}{\mu_2}, \dots, \frac{\mu_n}{\mu_{n-1}}, \sum_{j=1}^{n} \frac{\mu_j}{\mu_n} \cdot \frac{|a_{j-1}|}{|a_n|} \Big\},$$

so the roots of f_1 satisfy

$$|m - \theta_i| \ge |m| - |\theta_i| \ge |m| - A > |q|, \quad i = 1, \dots, t,$$

which by (1) gives the contradiction and completes the proof. ■

Proof of Theorem 1.11 In this case we use a classical result of Ballieu (see [1,11]) on the location of the roots of a complex polynomial:

https://doi.org/10.4153/CMB-2009-052-9 Published online by Cambridge University Press

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

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

This result follows immediately by using (3) for the transpose of $\mathcal{M}_{\tilde{f}}$.

Using again the same notations as in the proof of Lemma 1.1, 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. ■

3 Examples

(i) Let $f(X) = 1 - X + X^2 + X^3 + 191X^4 - X^5 - X^6 - X^7$, $m = 2$, $q = 1$, and $j = 4$. Since $f(2) = 2843$, which is a prime number, and

$$191 = |a_4| > (|m| + |q|)^{d_7 - d_4} \cdot \sum_{i \neq 4} |a_i| = 3^3 \cdot 7 = 189,$$

it follows by Corollary 1.3 that f is irreducible over $\mathbb{Q}$. We note that given an integer polynomial, one may obtain sharper irreducibility conditions by a suitable choice of the μ_i's in Theorem 1.2, rather than testing a single inequality as in Corollary 1.3.

(ii) Let $f(X) = p \cdot q + a_1 X + a_2 X^2 + \cdots + a_n X^n \in \mathbb{Z}[X]$, with $q a_n \neq 0$ and p a prime number. If $p > \sum_{i=1}^{n} |a_i| \cdot |q|^{i-1}$, then f must be irreducible over $\mathbb{Q}$. This follows immediately by taking $m = 0$ in Proposition 1.4. One such polynomial is $f(X) = 614 + 2X - 2X^2 - X^3 + X^4 - 6X^5 + 6X^6$. Here we have $p = 307$, $q = 2$, and $614 > \sum_{i=1}^{6} |a_i| 2^{i-1} = 612$, so f is an irreducible polynomial.

(iii) Let $k \geq 2$ and let $f(X) = a_0 + a_1 X + \ldots + a_n X^n \in \mathbb{Z}[X]$ be such that $|a_n| > |a_0| + |a_1| + \ldots + |a_{n-1}|$ and $f(2^k)$ is a prime number. Then the polynomial $f(X^k)$ is irreducible over $\mathbb{Q}$. Here we observe that the polynomial $f_k(X) = f(X^k)$ satisfies the hypotheses of Proposition 1.5 with $m = 2$ and $q = 1$, therefore being irreducible over $\mathbb{Q}$. For instance, for $f(X) = 1 + X + X^2 + X^3 - 3X^4 + 8X^5$ we have $f(2^3) = 250\,441$, which is a prime number, so the polynomial $f(X^3)$ is irreducible over $\mathbb{Q}$.

(iv) Let us take $f(X) = 1379 - 340X + 85X^2 + 21X^3 + 5X^4 + X^5$. Here $\sum_{i=0}^{5} a_i = 1151$, which is a prime number, and $|a_0| > \sum_{i=1}^{n} |a_i| 2^i$, so f is irreducible by Corollary 1.6.

(v) Let $f(X) = 1 + X + X^2 - X^3 - X^4 + X^5 - X^6 + X^7 + X^8$. Here we have $f(3) = 8167$, which is a prime number, so f is irreducible by Corollary 1.7.

(vi) If we take $\mu_j = 1$ for $j = 1, \ldots, n$ in Theorem 1.8, we see that a polynomial $f(X) = \sum_{i=0}^{n} a_i X^i \in \mathbb{Z}[X]$ with $a_0 a_1 \ldots a_n \neq 0$, $|a_0| < |a_1|$, and $2|a_{j-1}| < |a_j|$ for $j = 2, 3, \ldots, n$ is irreducible over $\mathbb{Q}$ if $f(m)$ is a prime number for an integer m with $|m| \geq 2$. One such polynomial is $f(X) = 1 - 2X - 5X^2 - 11X^3 - 23X^4 + 51X^5$, since $f(2) = 1153$, which is a prime number.

https://doi.org/10.4153/CMB-2009-052-9 Published online by Cambridge University Press

(vii) From Theorem 1.10 with $\mu_1 = \mu_2 = \dots = \mu_n = 1$ and $q = 1$ 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 $f(m)$ is a prime number for an integer m with $|m| > (|a_0|+|a_1|+\cdots+|a_n|)/|a_n|$, must be irreducible over $\mathbb{Q}$. Take for instance $f(X) = -2 - X + 2X^2 - 2X^3 - X^4 + X^5$ and $m = 11$. Here $f(11) = 143\,977$, which is a prime number, so f must be irreducible.

(viii) For a result related to Corollary 1.12, let us consider the polynomial $f(X) = 1 - X - X^2 + 11X^3 + 11X^4 + X^5 - 2X^6 + 11X^7$. Here $f(4) = 176\,557$, which is a prime number, and $|m| - |q| = 3$ while $\max_{0 \le i \le 6}(1 + |a_i|/|a_7|) = 2$, so f is an irreducible polynomial.

References

[1] R. Ballieu, *Sur les limitations des racines d'une équation algébrique.* Acad. Roy. Belg. Bull. Cl. Sci. (5) **33**(1947), 747–750.

[2] N. C. Bonciocat and A. Zaharescu, *Irreducible multivariate polynomials obtained from polynomials in fewer variables.* J. Pure Appl. Algebra **212**(2008), no. 10, 2338–2343.

[3] J. Brillhart, M. Filaseta and A. Odlyzko, *On an irreducibility theorem of A. Cohn*, Canad. J. Math. 33 (1981) no. 5, 1055–1059.

[4] V. F. Cowling and W. J. Thron, *Zero-free regions of polynomials.* Amer. Math. Monthly **61**(1954), 682–687.

[5] ———, *Zero-free regions of polynomials.* J. Indian Math. Soc. (N.S.) **20**(1956), 307–310.

[6] M. Filaseta, *A further generalization of an irreducibility theorem of A. Cohn.* Canad. J. Math. **34**(1982), no. 6, 1390–1395.

[7] ———, *Irreducibility criteria for polynomials with non-negative coefficients.* Canad. J. Math. **40**(1988), no. 2, 339–351.

[8] M. Fujiwara, *Über die obere Schranke des absoluten Betrages der Wurzeln einer algebraischen Gleichung*, Tôhoku Math. J. **10**(1916), 167–171.

[9] T. Kojima, *On a theorem of Hadamard's and its application.* Tôhoku Math. J. **5**(1914), 54–60.

[10] ———, *The limits of the roots of an algebraic equation.* Tôhoku Math. J. **11**(1917), 119–127.

[11] M. Marden, *Geometry of polynomials.* Mathematical Surveys and Monographs No. 3, American Mathematical Society, Providence, RI, 1966.

[12] O. Perron, Algebra. II *Theorie der algebraischen Gleichungen.* Walter de Gruyter & Co., Berlin, 1951.

[13] G. Pólya, G. Szegö, *Aufgaben und Lehrsätze aus der Analysis*, Springer-Verlag, Berlin, 1964.

[14] M. Ram Murty, *Prime numbers and irreducible polynomials.* Amer. Math. Monthly **109**(2002), no. 5, 452–458.

Institute of Mathematics, of the Romanian Academy, Bucharest 014700, Romania
e-mail: Anca.Bonciocat@imar.ro
Nicolae.Bonciocat@imar.ro

https://doi.org/10.4153/CMB-2009-052-9 Published online by Cambridge University Press