SIMPLE ARITHMETICAL CRITERIA FOR IRREDUCIBILITY OF POLYNOMIALS WITH INTEGER COEFFICIENTS

Natalio H. Guersenzvaig
Dept. of Mathematics, Universidad CAECE (Retired), Buenos Aires, Argentina
nguersenz@fibertel.com.ar

Received: 4/13/12, Revised: 11/17/12, Accepted: 1/7/13, Published: 1/25/13

Abstract

A simultaneous generalization of well-known arithmetical criteria for irreducibility in $\mathbb{Q}[X]$ of polynomials in $\mathbb{Z}[X]$, including a classical result of G. Pólya and G. Szegö, will be achieved via a general framework for that family of irreducibility criteria. A further generalization, which for any $f(X) \in \mathbb{Z}[X]$ provides an arithmetical function whose values are upper bounds for the number of irreducible factors of $f(X)$ in $\mathbb{Q}[X]$, will also be established.

1. Introduction

Let $Z \in \{\mathbb{Z}, \mathbb{Q}\}$ and let $\mathcal{U} = \{\pm 1\}$ or $\mathcal{U} = \mathbb{Z}$ according to whether $Z = \mathbb{Z}$ or $Z = \mathbb{Q}$, respectively. Let $f(X)$ denote an arbitrary polynomial in $\mathbb{Z}[X] \setminus \mathcal{U}$. We first remind the reader that $f(X)$ is called *reducible (irreducible) in* $Z[X]$, if there are (there are not, respectively) polynomials $g(X)$, $h(X)$ in $Z[X] \setminus \mathcal{U}$ satisfying $f(X) = g(X)h(X)$.

In this paper we focus our attention on a particular type of irreducibility criteria in $Z[X]$. Such results could be called *simple arithmetical criteria*, because they provide sufficient conditions for the irreducibility of $f(X)$ that only depend on the nature of the value $f(q)$ in a unique and conveniently chosen integer q. When $|f(q)| > 1$ we can write, possibly in several ways, $f(q) = \pm dp^e$, where d, p and e are positive integers with p prime. The most important criteria of this kind were established, in chronological order, by P. Stäckel (case $d = e = 1$), G. Pólya and G. Szegö (case $d = e = 1$), O. Ore (case $e = 1$), L. Weisner (general case), and M. Filaseta (case $e = 1$). A useful review of the known irreducibility criteria before 1935 is given in [6]; other results can be found in [13], and [18]. In spite of the different formulations of these results, including a generalization by the author of Pólya-Szegö's criterion, a careful scrutiny of their hypotheses allowed us to detect that besides the technical condition $p \nmid f'(q))^{e-1}$ introduced by Weisner in [21], which allows us to treat p^e like a prime number, similar sets of

hypotheses are satisfied by ρ, q and d, where ρ denotes a real parameter which is used to locate the zeros of $f(X)$ in the complex plane. As a result of such observations a general framework for expanded versions of these criteria will be established. Perhaps unexpectedly, an even more general result can be proved. Indeed, our generalization will be extended (in the last section of this paper) via a theorem that for any "f-admissible" triple (ρ, q, d) provides integer upper bounds for N_f, the number of irreducible factors of $f(X)$ in $\mathbb{Q}[X]$.

2. A General Framework for Simple Arithmetical Criteria of Irreducibility in $\mathbb{Z}[X]$

First, summarizing our analysis of the sets of hypotheses of the aforementioned irreducibility criteria, we introduce the notion of "admissible triple."

Definition 2.1. Let S be a nonempty subset of $\mathbb{R} \times \mathbb{Z}$ and let $\mathcal{Z}$ be a mapping defined in $S \times \mathbb{N}$ whose values $\mathcal{Z}(\rho, q, d)$ are subsets of $\mathbb{C}$. Let $\mathcal{F}$ be a function defined in $(\mathbb{Z}[X] \setminus \{0\}) \times S$ with values $\mathcal{F}(f, \rho, q)$ in the real interval $[1, +\infty)$. Let $f(X)$ be any nonzero polynomial in $\mathbb{Z}[X]$.

The triple $(S, \mathcal{Z}, \mathcal{F})$ will be called *f-admissible*, if for any $(\rho, q, d) \in S \times \mathbb{N}$ such that

$$d | f(q),\ q \notin \mathcal{Z}(\rho, q, d) \text{ and the zeros of } f(X) \text{ belong to } \mathcal{Z}(\rho, q, d)$$

the following condition is satisfied:

(**Condition** $\mathcal{A}$) for any polynomial $g(X) \in \mathbb{Z}[X]$ of positive degree dividing $f(X)$,

$$g(q) | d \implies |g(q)| > \mathcal{F}(f, \rho, q).$$

Most of the above criteria are related to the irreducibility of $f(X)$ in $\mathbb{Q}[X]$. In order to also include in our framework sufficient conditions for the irreducibility of $f(X)$ in $\mathbb{Z}[X]$ we recall that the greatest common divisor of the coefficients of $f(X)$, say $\mathrm{c}(f)$, is called *content* of $f(X)$ and that $f(X)$ is called *primitive* if $\mathrm{c}(f) = 1$. Notice now that the given definitions of irreducibility guarantee that $f(X)$ is irreducible in $\mathbb{Z}[X]$ if and only if

$$\text{either } f(X) = \pm p, \text{ or } f(X) \text{ is primitive and irreducible in } \mathbb{Q}[X]. \tag{1}$$

Our theoretical framework also includes sufficient conditions for the irreducibility of $f(X)$ in $\mathbb{Z}[X]$ without invoking explicitly the primitivity of $f(X)$, as described below.

Theorem 2.2. ((S,$\mathcal{Z}$,$\mathcal{F}$)–Irreducibility Criterion) *Let $f(X)$ be an arbitrary nonzero polynomial in $\mathbb{Z}[X]$ and let $(S,\mathcal{Z},\mathcal{F})$ be any f-admissible triple. Let $(\rho,q,d)\in S\times\mathbb{N}$ such that $d|f(q)$, $q\notin\mathcal{Z}(\rho,q,d)$ and the zeros of $f(X)$ belong to $\mathcal{Z}(\rho,q,d)$. Suppose also that*

$$d\le\mathcal{F}(f,\rho,q),\quad f(q)=\pm dp^e \text{ and } p\nmid(f'(q))^{e-1},$$

where p and e are positive integers with p prime. Then

$$f(X) \text{ is irreducible in } \mathbb{Q}[X] \iff f(X) \text{ has positive degree} \iff p\nmid c(f). \quad (2)$$

Moreover,

$$f(X) \text{ is irreducible in } \mathbb{Z}[X] \iff \gcd(d,c(f))=1. \quad (3)$$

Proof. First we will prove (2). Suppose $f(X)=g(X)h(X)$ with $g(X)$ and $h(X)$ in $\mathbb{Z}[X]$. Since the definition of irreducibility in $\mathbb{Q}[X]$ requires that $f(X)$ has positive degree, to complete the proof of the first equivalence we only need to show that one of the polynomials $g(X)$, $h(X)$ has degree zero.

From $g(q)h(q)=\pm dp^e$ it easily follows that there are nonnegative integers d_1,d_2,e_1,e_2, with $d=d_1d_2$ and $e=e_1+e_2$, such that $|g(q)|=d_1p^{e_1}$ and $|h(q)|=d_2p^{e_2}$. Certainly $e_1e_2=0$ if $e=1$. We also have $e_1e_2=0$ if $e>1$, because otherwise from $f'(q)=g'(q)h(q)+g(q)h'(q)$ we would obtain $p|(f'(q))^{e-1}$, a contradiction. Hence we can assume $e_1=0$, that is, $|g(q)|=d_1$. Then $g(X)$ is a constant polynomial, because otherwise (Condition $\mathcal{A}$) yields $|g(q)|>\mathcal{F}(f,\rho,q)$ against $d_1\le d\le\mathcal{F}(f,\rho,q)$.

On the other hand, it is clear that $p|c(f)$ if $f(X)$ is a constant polynomial. To prove the converse statement we assume $p|c(f)$. This clearly implies $p|f'(q)$, which combined with the hypothesis $p\nmid(f'(q))^{e-1}$ ensures $e=1$. Hence we get that $f(X)/p$ is a divisor of $f(X)$ satisfying $|f(q)/q|=d$. Then $f(X)$ is a constant polynomial, because otherwise (Condition $\mathcal{A}$) yields the contradiction $d>\mathcal{F}(f,\rho,q)$.

Finally, to prove (3), note that (2) guarantees that (1) is equivalent to

$$\text{either } f(X)=\pm p, \text{ or } f(X) \text{ has positive degree and } \gcd(d,c(f))=1,$$

and hence, via $f(q)=\pm dp^e$, to $\gcd(d,c(f))=1$. □

Next we will show that Weisner's hypothesis is unnecessary if d is appropriately chosen. In fact, a precise result can be established via the following definition:

Definition 2.3 Let a,b be arbitrary positive integers. The *b-part of a*, say $\delta(a,b)$, is defined by $\delta(a,b)=d_0\cdots d_{k-1}$, where $d_0=1$ and

$$d_j=\gcd\left(\frac{a}{d_0\cdots d_{j-1}},b\right) \text{ for } j=1,\dots,k-1.$$

Here k denotes the smallest positive integer with $d_k=1$.

It can be readily seen that we have defined $\delta(a,b)$ so that the following is true:

$$\delta(a,b) = \min\{c \in \mathbb{N} : c|a \text{ and } \gcd(a/c,b) = 1\}.$$

Now we can easily derive of Theorem 2.2 the following result.

Corollary 2.4. *Let $f(X)$ be an arbitrary primitive polynomial in $\mathbb{Z}[X]$ of positive degree and let $(S,\mathcal{Z},\mathcal{F})$ be any f-admissible triple. Let $(\rho,q,d) \in S\times\mathbb{N}$ such that $d|f(q)$, $\delta(|f(q)|,|f'(q)|)|d$, $q \notin \mathcal{Z}(\rho,q,d)$ and the zeros of $f(X)$ belong to $\mathcal{Z}(\rho,q,d)$. Suppose also that $d \le \mathcal{F}(f,\rho,q)$ and $f(q) = \pm dp^e$, where p and e are positive integers with p prime. Then $f(X)$ is irreducible in $\mathbb{Q}[X]$.*

Proof. The aforementioned property of $\delta(|f(q)|,|f'(q)|)$ and $\delta(|f(q)|,|f'(q)|)|d$ guarantees $\gcd(p^e,f'(q)) = \gcd(f(q)/d,f'(q)) = 1$, that is, $p \nmid f'(q)$. Then, as all hypotheses of Theorem 2.2 that are required to prove that $f(X)$ is irreducible in $\mathbb{Q}[X]$ are fulfilled, the proof is complete. □

In the next section, for a better understanding of Definition 2.1, the irreducibility criteria listed above will be conveniently reformulated. The admissible triples corresponding to the more general criteria will be presented in Section 5, after establishing our generalizations of the Pólya-Szegö criterion.

3. A Review of Simple Arithmetical Criteria and Related Facts

There are irreducible polynomials in $\mathbb{Z}[X]$ that can not represent infinitely many primes over the integers. For example, as an extreme case, the polynomial $f(X) = X^2+X+4$ is irreducible in $\mathbb{Z}[X]$ but $|f(q)| = q(q+1)+4$ is an even integer greater than 3 for any integer q. We recall now a conjecture of V. Bouniakowsky (see cite 5, p. 333) that would generalize the celebrated Dirichlet's Theorem on primes in arithmetic progressions (1837). This conjecture, which has not yet been proved or refuted, can be stated as follows.

Bouniakowsky's Conjecture. (1857) For any $f(X) \in \mathbb{Z}[X]$ of positive degree m that is irreducible in $\mathbb{Z}[X]$ there exist infinitely many integers q such that $f(q)/d(f)$ is a prime number, where $d(f)$ denotes the greatest common divisor of all the values of $f(X)$ over the integers.

Remark 3.1. (I) Bouniakowsky also gave a complicated procedure to compute $d(f)$. A better one was given in 1896 by K. Hensel (see [5], pp. 332, 334]) who proved, using the well-known Newton's Formula

$$f(q+k) = \sum_{j=0}^{\min\{k,m\}} \binom{k}{j} \Delta^j f(q),\ k=0,1,\ldots, \text{ where } \Delta^j f(q) = \sum_{i=0}^{j} (-1)^{j-i} \binom{j}{i} f(q+i),$$

that $d(f)$ is the greatest common divisor of the values of $f(X)$ in any $m+1$ consecutive integers, say $q, q+1, \ldots, q+m$.

(II) A stronger conjecture formulated in 1962 by Bateman and Horn (see [1]) would imply in the case $d(f)=1$ (see [12]) that

$$\pi(n,f) \underset{n\to\infty}{\sim} \frac{\mathrm{C}(f)}{m}\frac{n}{\log n}.$$

Here, $\pi(n,f)$ denotes the number of integers q with $1<q<n$ for which $|f(q)|$ is prime and

$$\mathrm{C}(f)=\prod_{p \text{ prime}} \frac{p-w(p)}{p-1},$$

where $w(p)$ stands for the number of solutions of the congruence $f(x)\equiv 0 \pmod{p}$.

The converse of the case $d(f)=1$ of the Bouniakowsky Conjecture is an easy consequence of the following theorem of P. Stäckel (see [20], Satz 1).

Stäckel's Theorem 1. (1918) *A reducible polynomial $f(X)\in\mathbb{Z}[X]$ of degree $m\geq 2$ can represent at most $2m$ prime numbers over the integers, and as soon as the absolute values of the integer q exceeds a certain limit, $f(q)$ will represent only composite numbers.*

Remark 3.2. In a relatively recent work ([4]) it is proved that $2m$ can be replaced by $m+2$ if $m\notin\{4,5\}$ and that there exist examples with m+1 instead of $m+2$. For m=4 or 5 the maximum possible value is 8.

Subsequently, Stäckel used a remark of O. Gmelin concerning the Fundamental Theorem of Algebra to establish the following result about the polynomials that represent prime numbers (see [20], Satz 7).

Stäckel's Theorem 7. (1918) *Let $f(X)\in\mathbb{Z}[X]$ and let $S=1+A$, where A denotes the maximum of the absolute values of the coefficients of $f(X)$. If there is an integer q with $|q|>S$ for which $f(q)$ is a prime number, then $f(X)$ is irreducible in $\mathbb{Z}[X]$.*

Remark 3.3. It should be noted that S constitutes the greatest possible value of a well-known Cauchy's upper bound for the absolute values of the zeros of $f(X)$, namely, $\rho_0=1+(A/|a_n|)$, where a_n denotes the leading coefficient of $f(X)$ (see [11], Theorem (27, 2)). Previously, without using the Fundamental Theorem of Algebra, Stäckel gave for the case $n=\deg(f)\geq 2$ (see [20], Satz 6) the value

$$S=2+\frac{An!(n-1)^{(n^2+n+2)/2}}{1!\cdots(n-1)!}.$$

Stäckel's Theorem 7 was improved by G. Pólya and G. Szegö through the following result (see [15], **127**, pp. 137, 350-351, or [17], **127**, pp. 130, 330).

Pólya-Szegö's Theorem. (1925) *Let $f(X)$ be an arbitrary polynomial in $\mathbb{Z}[X]$. Assume that there exists an integer q such that the zeros of $f(X)$ lie in the half*

plane $\Re(z) < q - \frac{1}{2}$, $f(q-1) \neq 0$ *and* $f(q) = p$, *where* p *is a prime number. Then* $f(X)$ *is irreducible in* $\mathbb{Z}[X]$.

Nine years later O. Ore gave a different generalization of Stäckel's Theorem 7 establishing sufficient conditions for the irreducibility in $\mathbb{Q}[X]$ of the polynomials in $\mathbb{Z}[X]$ that represent multiples of primes (see [14], Satz 5).

Ore's Theorem. (1934) *Let* $f(X)$ *be an arbitrary polynomial in* $\mathbb{Z}[X]$ *of degree* $n \geq 2$. *Assume that there exist a real number* ρ, *an integer* q *and a positive integer* d *such that* $\rho \geq 1$, $d|f(q)$ *and the zeros of* $f(X)$ *are outside of the disk* $|z - q| \leq \rho$. *Suppose also that* $d \leq \rho$ *and* $f(q) = dp$, *where* p *is a prime number. Then* $f(X)$ *is irreducible in* $\mathbb{Q}[X]$.

Remark 3.4. An equivalent result that does not use the real parameter ρ can be established replacing the hypotheses

$$\textit{the zeros of } f(X) \textit{ are outside of the disk } |z - q| \leq \rho, \quad d \leq \rho$$

by a single statement, namely,

$$\textit{the zeros of } f(X) \textit{ are outside of the disk } |z - q| \leq d.$$

In the last paragraph of [14] Ore says that the sufficient conditions of irreducibility of the previous theorem can be extended in distinct directions. This task was accomplished, almost simultaneously, by L. Weisner who established necessary conditions for the reducibility of the polynomials that represent multiples of prime powers (see [21]). In particular, besides establishing the case $q = 0$ of Ore's Theorem, Weisner derives from its first two theorems a result that we state as an irreducibility criterion in the following equivalent way, where $\mathbb{Z}_{(1)}[X] = \mathbb{Z}[X] \setminus \{-1, 1\}$ and $\mathbb{Z}_{(2)}[X]$ stands for the set of polynomials in $\mathbb{Z}_{(1)}[X]$ without rational roots.

Weisner's Theorem 3. (1934) *Let* $v \in \{1, 2\}$ *and let* $f(X)$ *be an arbitrary polynomial in* $\mathbb{Z}_{(v)}[X]$ *of degree* $n \geq 2$ *and leading coefficient* a_n. *Assume that there exist a real number* ρ, *an integer* q *and a positive integer* d *such that* $\rho \geq 1$, $|q| \geq \rho + 1$, $d|f(q)$ *and the zeros of* $f(X)$ *are in the disk* $|z| < \rho$. *Suppose also that*

$$\text{(A) } d \leq (|q| - \rho)^v \quad \textit{or} \quad \text{(B) } p^e \geq |a_n|(|q| + \rho)^{n-v},$$

$$f(q) = \pm\, dp^e \quad \textit{and} \quad p \nmid (f'(q))^{e-1},$$

where p *and* e *are positive integers with* p *prime. Then* $f(X)$ *is irreducible in* $\mathbb{Q}[X]$.

Remark 3.5. (I) Case $v = e = 1$ of part (A) was also established by Ore in the last paragraph of [14] and rediscovered several times in the last forty years; see, for example, [2], Theorem 1 and [9], Theorem 1.

(II) Since $p^e \geq |a|(|q| + \rho)^{n-v}$ and $d \leq |f(q)|/(|a_n|(|q| + \rho)^{n-v})$ are equivalent inequalities, we can rewrite

$$(\mathrm{A})\, d \le (|q|-\rho)^v \;\; or \;\; (\mathrm{B})\, p^e \ge |a_n|(|q|+\rho)^{n-v}$$

as

$$d \le \max\left\{(|q|-\rho)^v,\, |f(q)|/(|a_n|(|q|+\rho)^{n-v})\right\}.$$

More recently, using a well-known bound for the absolute value of the zeros with positive real part of the polynomials in $\mathbb{R}[X]$ with nonnegative coefficients (say $|z| < \rho_1$; see, for example, [16], (**24**)), M. Filaseta improves a previous result of J. Brillhart, M. Filaseta and A. Odlizko (see [3], Theorem 4) establishing the following theorem (see [7], Theorem 4]).

Filaseta's Theorem 1. (1982) *Let $f(X) = \sum_{j=0}^{m} a_j X^j$ be any polynomial in $\mathbb{Z}_{(2)}[X]$ with $a_m > 0$ and $a_{m-1} \ge 0$. Let $\rho_1 = (1+\sqrt{4M+1})/2$, where $M = \max_{k=0,1,\ldots,m-2} |a_k/a_m|$. Let q be any integer and let d be any positive integer such that $q \ge \rho_1 + 1$ and $d|f(q)$. Suppose also that $d \le (q-\rho_1)^2$ and $f(q) = dp$, where p is a prime number. Then $f(X)$ is irreducible in $\mathbb{Q}[X]$.*

Filaseta also established the following result concerning the construction of irreducible polynomials from multiples of primes (see [7], Theorem 2; case $d = 1$ can be found in Corollary 2 of [3]; see also [19]).

Filaseta's Theorem 2. (1982) *Let p, d, q be positive integers, with p prime and $dp \ge q > d$. Let $f(X)$ denote the polynomial in $\mathbb{Z}[X]$ which is obtained replacing q by X in the representation of dp in base q. Then $f(X)$ is irreducible in $\mathbb{Q}[X]$.*

Remark 3.6. Other important results of Filaseta for polynomials in $\mathbb{Z}[X]$ with nonnegative coefficients, also related to the case $f(q) = dp$, can be found in [8]. In particular, the preceding theorem is improved by Theorem 5 which admits much larger coefficients of relatively low order. It should be also noted that to prove this theorem the case $\rho = \sqrt{d}$ of Ore's Theorem (which is proved in Lemma 1) is used.

4. Generalizations of the Pólya-Szegö Theorem

In this section we generalize Pólya-Szegö's Theorem, which according to the best knowledge of the author has not been done yet. We first present a result similar to Ore's Theorem (see Remark 3.4). Indeed, Pólya-Szegö's Theorem is equivalent to the case $d = 1$ of the following result (see Remark 2.3).

Theorem 4.1. *Let $f(X)$ be an arbitrary polynomial in $\mathbb{Z}_{(1)}[X]$. Assume that there exist an integer q and a positive integer d such that $d|f(q)$, $\gcd(d, c(f)) = 1$ and the zeros of $f(X)$ lie in the punctured half plane $\Re(z) < q - \frac{d}{2}$, $z \ne q-d$. Suppose also that $f(q) = dp$, where p is a prime number. Then $f(X)$ is irreducible in $\mathbb{Z}[X]$.*

Remark 4.2. We can not conclude in all cases that $f(X)$ is irreducible in $\mathbb{Z}[X]$ if the fraction $d/2$ is replaced by d/k, where k is any real number greater than 2. In this situation we have, for example, the reducible polynomial

$$f(X) = ((X-q)^{2n+1} + p)(p(X-q) + d),$$

where q, n, p and d are arbitrary positive integers with p prime and $d < p < k$. Indeed, $f(X)$ is primitive and has its zeros in the half plane $\Re(z) \leq q - \frac{d}{p} < q - \frac{d}{k}$, also satisfying $f(q-d) = d(p + (-d)^{2n+1})(1-p) \neq 0$ and $f(q) = dp$.

A generalization of the above theorem using Weisner's condition can be established. Indeed, Theorem 4.1 is equivalent to the case $v = e = 1$ of the following result.

Theorem 4.3. (Generalized Pólya-Szegö's Theorem (1)) *Let $v \in \{1, 2\}$ and let $f(X)$ be an arbitrary polynomial in $\mathbb{Z}_{(v)}[X]$. Assume that there exist an integer q and a positive integer d such that $d|f(q)$, $\gcd(d, c(f)) = 1$ and the zeros of $f(X)$ are in the punctured half plane*

$$\Re(z) < q - \min\left\{\tfrac{d}{2},\ \sqrt[v]{d}\right\},\ z \neq q - d.$$

Suppose also that $f(q) = \pm\, dp^e$ and $p \nmid (f'(q))^{e-1}$, where p and e are positive integers with p prime. Then $f(X)$ is irreducible in $\mathbb{Z}[X]$.

Now, since for any real number ρ,

$$\rho \leq q - \min\left\{\frac{d}{2},\ \sqrt[v]{d}\right\} \text{ if and only if } d \leq \max\{2(q-\rho),\ (q-\rho)^v\},$$

we state our final generalization of the Pólya-Szegö Theorem rewriting Theorem 4.3 in the following way, which became the model for Theorem 2.2.

Theorem 4.4. (Generalized Pólya-Szegö's Theorem (2)) *Let $v \in \{1, 2\}$ and let $f(X)$ be an arbitrary polynomial in $\mathbb{Z}_{(v)}[X]$. Assume that there exist a real number ρ, an integer $q \geq \rho + \frac{1}{2}$ and a positive integer d such that $d|f(q)$ and the zeros of $f(X)$ are in the punctured half plane $\Re(z) < \rho$, $z \neq q - d$. Suppose also that*

$$d \leq \max\{2(q-\rho),\ (q-\rho)^v\},\ f(q) = \pm\, dp^e,\ \text{and}\ p \nmid (f'(q))^{e-1},$$

where p and e are positive integers with p prime. Then

$$f(X) \text{ is irreducible in } \mathbb{Q}[X] \iff f(X) \text{ has positive degree.} \tag{2*}$$

Moreover,

$$f(X) \text{ is irreducible in } \mathbb{Z}[X] \iff \gcd(d, c(f)) = 1. \tag{3*}$$

Remark 4.5. Because $|z| < \rho$ implies $\Re(z) < \rho$, Weisner's Theorem 3 (A) can also be derived of Theorem 4.4 (the proof of the case $q < 0$ requires to use $f^*(X) = f(-X)$ and $q^* = -q$ instead of $f(X)$ and q, respectively). It is also clear that Filaseta's Theorem 1 is included in the case $\rho = \rho_1$, $e = 1$, $v = 2$ of Theorem 4.4.

A proof of Theorem 4.4 will be given in the next section. Now we use it to build irreducible polynomials from multiples of prime powers. Given any integer $q \geq 2$ we shall say that a nonzero polynomial in $\mathbb{Z}[X]$ is a *q-polynomial* if all its coefficients are in the interval $0 \leq x < q$. The following lemma, which will be proved in Appendix A, gives a very simple upper bound for the real part of the zeros of any q-polynomial.

Lemma 4.6. *For every integer $q \geq 2$, the zeros of any q-polynomial in $\mathbb{Z}[X]$ lie in the half plane $\Re(z) < \sqrt{q}$.*

A proof of the following theorem will be given in Appendix B.

Theorem 4.7. *Let a, d, p and e be arbitrary positive integers, with $a \geq 2$ and p prime, such that $d < q < dp^e$, where $q = pa$. Let $f(X)$ denote the polynomial in $\mathbb{Z}[X]$ which is obtained replacing q by X in the representation of dp^e in base q. Then*

$$f(X) \text{ is irreducible in } \mathbb{Q}[X] \text{ if } q \notin \bigcup_{1 \leq j < dp^{e-1}} \left(\frac{dp^e}{pj+1}, \frac{dp^e}{pj} \right]. \tag{4}$$

In particular,

$$f(X) \text{ is irreducible in } \mathbb{Q}[X] \text{ if } a^2 | (p-1) \text{ and } a \nmid d. \tag{5}$$

Furthermore,

$$\text{if } a^2 | (p-1) \text{ and } \gcd(d, [d/a]q) = 1, \text{ then } f(X) \text{ is irreducible in } \mathbb{Z}[X]. \tag{6}$$

Thus, for example, considering the simplest case of the above theorem, namely, $a = 2$, $p = 5$ and $d = 1$, we get that all polynomials that are obtained from the integer powers of 5, that is, $5,\ 2X + 5,\ X^2 + 2X + 5,\ 6X^2 + 2X + 5, \ldots$, are irreducible in $\mathbb{Z}[X]$.

5. Main Admissible Triples

In this section we present the admissible triples associated with the missing generalization of Ore's Theorem, Weisner's Theorem 3 (according to (II) of Remark 3.5) and Theorem 4.4, our final generalization of the Pólya and Szegö Theorem. By comparing the definitions below with the corresponding statements it can be readily seen that these theorems are immediate consequences of Theorem 2.2 and the following result.

Theorem 5.1. *Let $v \in \{1, 2\}$ and let $f(X)$ be an arbitrary polynomial in $\mathbb{Z}_{(v)}[X]$. Assume that $f(X)$ has degree n and leading coefficient a_n. Then the following triples*

are f-admissible:

$$(S,\mathcal{Z},\mathcal{F})_v^{\mathrm{Ore}}:\begin{cases} S=\{(\rho,q)\in\mathbb{R}\times\mathbb{Z}:\rho\geq 1\}\\ \mathcal{Z}(\rho,q,d)=\begin{cases}\{z\in\mathbb{C}:|q-z|>\rho\} & \text{if } v=1\\ \{z\in\mathbb{C}\setminus\mathbb{Q}:|q-z|>\rho\} & \text{if } v=2\end{cases}\\ \mathcal{F}(f,\rho,q)=\rho^v,\end{cases}$$

$$(S,\mathcal{Z},\mathcal{F})_v^{\mathrm{Weisner}}:\begin{cases} S=\{(\rho,q)\in\mathbb{R}\times\mathbb{Z}:\rho\geq 1,|q|\geq\rho+1\}\\ \mathcal{Z}(\rho,q,d)=\begin{cases}\{z\in\mathbb{C}:|z|<\rho\} & \text{if } v=1\\ \{z\in\mathbb{C}\setminus\mathbb{Q}:|z|<\rho\} & \text{if } v=2\end{cases}\\ \mathcal{F}(f,\rho,q)=\max\left\{(|q|-\rho)^v,|f(q)|/(|a_n|(|q|+\rho)^{n-v})\right\},\end{cases}$$

$$(S,\mathcal{Z},\mathcal{F})_v^{\mathrm{P\&S}}:\begin{cases} S=\left\{(\rho,q)\in\mathbb{R}\times\mathbb{Z}:q\geq\rho+\frac{1}{2}\right\}\\ \mathcal{Z}(\rho,q,d)=\begin{cases}\{z\in\mathbb{C}\setminus\{q-d\}:\Re(z)<\rho\} & \text{if } v=1,\ d\leq 2(q-\rho)\\ \{z\in\mathbb{C}\setminus\mathbb{Z}:\Re(z)<\rho\} & \text{if } v=1,\ d>2(q-\rho)\\ \{z\in\mathbb{C}\setminus\mathbb{Q}:\Re(z)<\rho\} & \text{if } v=2\end{cases}\\ \mathcal{F}(f,\rho,q)=\max\{2(q-\rho),(q-\rho)^v\}.\end{cases}$$

Our proof that the triple $(S,\mathcal{Z},\mathcal{F})_v^{\mathrm{P\&S}}$ is f-admissible depends on the following lemma (which constitutes the core of the original proof of Pólya-Szegö's Theorem; see [17], **127**, p. 330).

Lemma 5.2. *Let $G(X)$ be an arbitrary nonzero polynomial in $\mathbb{Z}[X]$. Let $\rho\in\mathbb{R}$ such that the zeros of $G(X)$ are in the half plane $\Re(z)<\rho$ and let $q\in\mathbb{Z}$, with $q\geq\rho+\frac{1}{2}$, such that $G(q-1)\neq 0$ and $G(q)=\pm 1$. Then $G(X)=\pm 1$.*

Proof. Clearly we only need to prove that $G(X)$ is a constant polynomial. On the contrary suppose that $G(X)$ has positive degree. It easily follows from our hypotheses that the zeros of $G(X+q-\frac{1}{2})$ lie in the half plane $\Re(z)<0$, so all its significant coefficients have the same sign. Therefore $|G(-x+q-\frac{1}{2})|<|G(x+q-\frac{1}{2})|$ for any positive real number x. Hence, letting $x=1/2$, we get the contradiction $1\leq|G(q-1)|<|G(q)|=1$. □

We can now give a more simple proof of Theorem 5.1.

Proof. Note first that the triples previously defined satisfy the basic specifications of Definition 2.1. Let $(\rho,q,d)\in S\times\mathbb{N}$ with $d|f(q)$ such that the zeros of $f(X)$ belong to $\mathcal{Z}(\rho,q,d)$, and let $g(X)$ be an arbitrary polynomial of positive degree in $\mathbb{Z}[X]$ that divides $f(X)$. Assume that $g(X)$ has degree m (so that $m\geq v$), leading coefficient c_m, and zeros $z_1,\ldots,z_m$. To prove that $g(X)$ satisfies (Condition $\mathcal{A}$) we will show that in each case at least one of the two statements $|g(q)|>\mathcal{F}(f,\rho,q)$ and $g(q)\nmid d$ holds.

In the first place we will prove that $|g(q)|>\mathcal{F}(f,\rho,q)$ for the first two triples. For $(S,\mathcal{Z},\mathcal{F})_v^{\mathrm{Ore}}$ we have,

$$|g(q)| = |c_m| \prod_{j=1}^{m} |q - z_j| \geq \prod_{j=1}^{m} |q - z_j| > \rho^m \geq \rho^v.$$

Considering $(S, \mathcal{Z}, \mathcal{F})_v^{\text{Weisner}}$, in the case $(|q|-\rho)^v > |f(q)|/(a|(|q|+\rho)^{n-v})$ we have,

$$|g(q)| = |c_m| \prod_{j=1}^{m} |q - z_j| \geq \prod_{j=1}^{m} ||q| - |z_j|| > (|q| - \rho)^m \geq (|q| - \rho)^v.$$

For the remaining case, assuming that $h(X) := f(X)/g(X)$ has leading coefficient b and roots $z_{m+1}, \ldots, z_n$ we have,

$$\frac{|f(q)|}{|a_n|(|q|+\rho)^{n-v}} \leq \frac{|g(q)||h(q)|}{|b|(|q|+\rho)^{n-v}} = \frac{|g(q)|\prod_{j=m+1}^{n}|q - z_j|}{(|q|+\rho)^{n-v}} < \frac{|g(q)|}{(|q|+\rho)^{m-v}} \leq |g(q)|.$$

Then it only remains to consider the triple $(S, \mathcal{Z}, \mathcal{F})_v^{\text{P\&S}}$. In the first place we prove that $g(q) \nmid d$ if $d/2 \leq q - \rho$.

On the contrary, suppose $d/2 \leq q - \rho$ and $g(q)|d$. Let $G(X) = g(dX + q)/|g(q)|$. From $g(q)|d$ we get $G(X) \in \mathbb{Z}[X]$. Clearly $G(0) = \pm 1$. Note also that for any complex root z of $G(X)$ we have $d\Re(z) + q < \rho$, so $\Re(z) < -(q - \rho)/d \leq -1/2$. On the other hand, $f(q - d) \neq 0$ implies $G(-1) = g(q - d)/|g(q)| \neq 0$. Therefore, since Lemma 5.2 applies to $G(X)$ with $\rho = -1/2$ and $q = 0$, we have $G(X) = \pm 1$ which means that $g(X)$ is a constant polynomial, a contradiction.

Now assume $d/2 > q - \rho$. We shall prove that $|g(q)| > \max\{2(q - \rho), (q - \rho)^v\}$. Notice that

$$\max\{2(q-\rho), (q-\rho)^v\} = \begin{cases} (q-\rho)^2 & \text{if } v = 2 \text{ and } q - \rho > 2 \\ (q-\rho)^2 = 2(q-\rho) & \text{if } v = 2 \text{ and } q - \rho = 2 \\ 2(q-\rho) & \text{if } v = 1 \text{ or } q - \rho < 2. \end{cases}$$

In the first place we suppose $m=1$, so $v = 1$. In this situation we have $|c_1| \geq 2$, because otherwise $g(X)$ has an integer root against the definition of $\mathcal{Z}(\rho, q, d)$. Therefore, $|g(q)| = |c_1||q - z_1| > 2|q - \rho| = 2(q - \rho) = \max\{2(q - \rho), (q - \rho)^v\}$.

We assume then that $m \geq 2$. Note that for any real $t \geq \rho$ all the significant coefficients of $g(X+t)$ have the same sign. Hence, letting $t = \rho$, $X = q - t$ we easily get,

$$|g(q)| > |c_m|(q-\rho)^m \geq (q-\rho)^m \geq \begin{cases} (q-\rho)^2 & \text{if } v = 2 \text{ and } q - \rho > 2 \\ (q-\rho)^2 = 2(q-\rho) & \text{if } q - \rho = 2 \\ 2(q-\rho) & \text{if } v = 1 \text{ and } q - \rho > 2, \end{cases}$$

which proves that $|g(q)| > \max\{2(q - \rho), (q - \rho)^v\}$ in the case $q - \rho \geq 2$.

Thus it only remains to show that $|g(q)| > 2(q-\rho)$ when $q-\rho < 2$. As $q-\rho \geq 1/2$ and

$$\left[\tfrac{1}{2}, 2\right) = \left[\tfrac{1}{2}, 1\right) \cup \left[1, \tfrac{3}{2}\right) \cup \left[\tfrac{3}{2}, 2\right),$$

it will be sufficient to prove that for $k = 1, 2, 3$,

$$q - \rho \in [k/2, (k+1)/2) \text{ implies } |g(q)| > k.$$

This holds for $k=1$ because otherwise Lemma 5.2 applies to $G(X)=g(X)$ giving the contradiction $g(X)=\pm 1$. Then suppose $k\in\{2,3\}$. Notice that $g^{(j)}(q-1)/j!$ and $2^{m-j}g^{(j)}\big(q-\frac{3}{2}\big)/j!$ are integer numbers for $j=0,1,\ldots,m$. Consequently,

$$\begin{aligned}|g(q)| &= \sum_{j=0}^{m}\left|\frac{g^{(j)}\big(q-\frac{k}{2}\big)}{j!}\right|\left(\frac{k}{2}\right)^{j}\\ &= \begin{cases}\sum_{j=0}^{m}\left|\dfrac{g^{(j)}(q-1)}{j!}\right| & \text{if } k=2\\ \dfrac{1}{2^m}\sum_{j=0}^{m}\left|\dfrac{2^{m-j}g^{(j)}\big(q-\frac{3}{2}\big)}{j!}\right|3^j & \text{if } k=3\end{cases}\\ &\geq \begin{cases}\sum_{j=0}^{m}1=m+1>2 & \text{if } k=2\\ \dfrac{1}{2^m}\sum_{j=0}^{m}3^j=\left(\dfrac{3}{2}\right)^{m+1}-\dfrac{1}{2^{m+1}}\geq\left(\dfrac{3}{2}\right)^{3}-\dfrac{1}{8}>3 & \text{if } k=3,\end{cases}\end{aligned}$$

as we wanted to show. □

6. On the Number of Irreducible Factors of the Polynomials in $\mathbb{Z}[X]$

In this section we will extend Theorem 2.2 via a theorem that for any polynomial $f(X)\in\mathbb{Z}[X]$ of positive degree and any "f-admissible triple" (ρ,q,d) yields an integer upper bound for N_f, the number of irreducible factors of $f(X)$ in $\mathbb{Q}[X]$ (multiplicities counted). Better bounds for the number of distinct irreducible factors of $f(X)$ in $\mathbb{Q}[X]$ will be obtained under certain additional hypotheses which guarantee that $f(X)$ is *square free*, which means that there does not exist a polynomial $k(X)\in\mathbb{Z}[X]$ of positive degree such that $k^2(X)|f(X)$.

Remark 6.1. In general, since $f(X)$ is square free if and only if $f(X)$ and $f'(X)$ have no common divisors of positive degree in $\mathbb{Z}[X]$, to obtain better estimates of the number of distinct irreducible factors of $f(X)$ in $\mathbb{Q}[X]$ we should replace $f(X)$ by its *square free part*, say $f_{\text{sqf}}(X)$, defined by

$$f_{\text{sqf}}(X)=\frac{f(X)}{\gcd(f(X),f'(X))},$$

where gcd stands for the greatest common divisor in $\mathbb{Z}[X]$ (an algorithm to compute it can be found in [13]). Such denomination is justified by the fact that $f_{\text{sqf}}(X)$ is the product of the different irreducible factors of $f(X)$ in $\mathbb{Z}[X]$ of positive degree, so that $f_{\text{sqf}}(X)$ is also primitive. Furthermore, in order to also diminish the computational cost of factoring large values of $|f(q)|$, it is convenient to work separately with the nonconstant components $P_1(X),\ldots,P_n(X)$ of the so-called *square free factorization* of $f(X)$,

$$f(X) = P_1(X)P_2^2(X)\cdots P_n^n(X),\ n = \deg(f),$$

which are square free and pairwise coprime polynomials in $\mathbb{Z}[X]$ (so $f_{\mathrm{sqf}}(X) = P_1(X)P_2(X)\cdots P_n(X)$). This can be done using, for example, the well-known Tobey-Horowitz algorithm, which is described together with a new procedure in [10].

Some definitions are needed to establish the bounds for N_f associated to a suitable triple (ρ, q, d). First we define two closely related counting functions which will be used to estimate the maximum number of irreducible factors of positive degree that can have a divisor of $f(X)$ in $\mathbb{Z}[X]$, say $g(X)$, satisfying $g(q)|d$.

Definition 6.2. Let d be a positive integer and let x be a real number, $x \geq 1$. Let $\Delta_x(d) = \Delta_x^*(d) = 0$ if $d \leq x$. Otherwise,

(a) $\Delta_x(d)$ denotes the largest positive integer k for which we can write $d = d_1 \cdots d_k$ with $d_j > x$ for $j = 1, \ldots, k$;

(b) $\Delta_x^*(d)$ denotes the largest positive integer k for which we can write $d = d_1 \cdots d_k$ with $d_1, \ldots, d_k$ pairwise coprime and $d_j > x$ for $j = 1, \ldots, k$.

Remark 6.3. Given the factorization $1 < d = p_1^{e_1} \cdots\ p_t^{e_t}$, with $p_1^e < \cdots < p_t^{e_t}$, it is clear that $\Delta_x^*(d) \leq t$ and $\Delta_x(d) \leq e_1 + \cdots + e_t$. It can also be shown without difficulty that $\Delta_x(d) < \log_x d$ if $x > 1$. Hence, for any $f(X) \in \mathbb{Z}_{(v)}[X]$ with $v \in \{1, 2\}$ and any of the f-admissible triples considered in Theorem 5.1, from the case $d = |f(q)|$, $x = \mathcal{F}(f, \rho, q)$ it can be readily deduced that for any q sufficiently large, $\Delta_{\mathcal{F}(f,\rho,q)}(|f(q)|) \leq \deg(f)/v$.

Next we present a quantitative version of Weisner's condition $p \nmid (f'(q))^{e-1}$, which will be used to estimate the maximum number of irreducible factors of positive degree that can have a divisor of $f(X)$ in $\mathbb{Z}[X]$, say $h(X)$, satisfying $h(q)|(f(q)/d)$.

Let $\Pi(a)$ denote the set of positive prime divisors of an arbitrary nonzero integer a. For each $p \in \Pi(a)$ let $e_p = e_p(a)$ be the largest positive integer k satisfying $p^k|a$. As usual, a is called *square free* if $e_p = 1$ for each $p \in \Pi(a)$. The *square free part of* a, say $\mathrm{sqf}(a)$, is defined as the product of the primes $p \in \Pi(a)$ with $e_p = 1$.

Definition 6.4. Let $f(X)$ be an arbitrary primitive polynomial in $\mathbb{Z}[X]$, and let q, d be any integers such that $f(q) \neq 0$ and $d|f(q)$. For each $p \in \Pi(f(q)/d)$ we define:

$$r_p(f, q) = \min\left\{k \in \mathbb{N} : p \nmid \left(\frac{f^{(k)}(q)}{k!}\right)^{e_p - 1}\right\}.$$

It should be noted that $r_p(f, q)$ is a well defined integer belonging to the set $\{1, \ldots, \deg(f)\}$. Indeed, $r_p(f, q) = 1$ if $e_p = 1$, and for $e_p \geq 2$ the supposition $p|f^{(k)}(q)/k!$ for $k = 1, \ldots, n - \deg(f)$ implies $p|f(X)$, via

$$f(X) = f(q) + f'(q)(X - q) + \cdots + \frac{f^{(n)}(q)}{n!}(X - q)^n,$$

which contradicts that $f(X)$ is primitive.

Now, to shorten the proof of the main theorem of this section, we establish a technical lemma which actually constitutes the part of such theorem that does not depend on admissibility.

Lemma 6.5. *Let $h(X)$ be a primitive polynomial in $\mathbb{Z}[X]$ and let q be any integer with $h(q) \neq 0$. Suppose that d_h is a positive divisor of $h(q)$ such that there is no polynomial $k(X)$ in $\mathbb{Z}[X]$ of positive degree satisfying $k(X)|h(X)$ and $k(q)|d_h$. Then*

$$N_h \leq \sum_{p\in\Pi(h(q)/d_h)} r_p(h,q). \tag{7}$$

Furthermore,

$$\sum_{p\in\Pi(h(q)/d_h)} r_p(h,q) = \#(\Pi(h(q)/d_h)) \iff \gcd(h(q)/d_h, h'(q))|\mathrm{sqf}(h(q)/d_h). \tag{8}$$

Proof. Let $\Pi = \Pi(h(q)/d_h)$ and, for each $p \in \Pi$, let $e_p = e_p(h(q)/d_h)$, $r_p = r_p(h,q)$.

Proof of (7). In case $|h(q)| = 1$ we have $N_h = 0 = \#(\Pi) = \sum_{p\in\Pi} r_p$. Now assume $|h(q)| \neq 1$. Thus $h(X)$ has positive degree and $t := \#(\Pi) \geq 1$. Let $\Pi = \{p_1, \ldots, p_t\}$, $e_j = e_{p_j}$ and $r_j = r_{p_j}$ for $j = 1, \ldots, t$. Thus we can write $|h(q)| = d_h p_1^{e_1} \ldots p_t^{e_t}$ and $h(X) = h_1(X) \cdots h_{N_h}(X)$, where each $h_j(X)$ has positive degree and is irreducible in $\mathbb{Z}[X]$. Because $h_j(q) \nmid d_h$ for $j = 1, \ldots, N_h$ we can assume $|h_j(q)| = d_j p_j^*$, where the d_j's are positive integers with $d_1 \cdots d_{N_h} = d_h$ and the p_j^*'s are integers greater than 1 with $p_1^* \cdots p_{N_h}^* = p_1^{e_1} \ldots p_t^{e_t}$.

We now define two polynomial sequences in $\mathbb{Z}[X]$, say $P_0(X), \ldots, P_t(X)$ and $H_1(X), \ldots, H_t(X)$. The $P_j(X)$'s are recursively defined starting with $P_0(X) = 1$. For $1 \leq j \leq t$ the polynomial $P_j(X)$ is defined as the product of all polynomials $h_k(X)$ with $k \in \{1, \ldots, N_h\}$ that are relatively prime to $P_0(X) \cdots P_{j-1}(X)$ and satisfy $p_j | p_k^*$. Notice that $h(X) = P_1(X) \cdots P_t(X)$. On the other hand we define $H_j(X)$ for $j \in \{1, \ldots, t\}$ as the product of all polynomials $h_k(X)$ with $k \in \{1, \ldots, N_h\}$ that satisfy $p_j | p_k^*$. It is clear that each $P_j(X)$ divides $H_j(X)$. Therefore, letting $N_j = N_{H_j}$ it will be enough to prove that $N_j \leq r_j,\ j = 1, \ldots, t$.

Let $j \in \{1, \ldots, t\}$. We can write $|H_j(q)| = \delta p_j^{e_j}$ for some $\delta \mid d_h \prod_{\substack{1\leq i\leq t \\ i\neq j}} p_i^{e_i}$. From $|h(q)|/d_h = p_1^{e_1} \ldots p_t^{e_t}$ and the definition of $H_j(X)$ we easily get $N_j \leq e_j$. Hence, to prove $N_j \leq r_j$, we can suppose $r_j < e_j$. Assume $H_j(X) = Q_1(X) \cdots Q_{N_j}(X)$, where each $Q_k(X)$ is an irreducible polynomial in $\mathbb{Z}[X]$. By definition of H_j we can write $|Q_k(q)|$ in the form $|Q_k(q)| = \delta_k p_j^{\epsilon_k}$, where ϵ_k, δ_k are positive integers with $e_j = \epsilon_1 + \cdots + \epsilon_{N_j}$ and $\delta = \delta_1 \cdots \delta_{N_j}$. Let $G_j(X) = h(X)/H_j(X)$ and let $r_{jk} = r_{p_j}(Q_k, q)$ for $k = 1, \ldots, N_j$. Hence, $h(X) = G_j(X) Q_1(X) \cdots Q_{N_j}(X)$.

From Leibniz's Formula for the successive derivatives of a product of polynomials we obtain

$$\frac{h^{(k)}(q)}{k!} = \sum_{\substack{k_0+k_1+\cdots+k_m=k \\ \text{each } k_i \geq 0}} \frac{G_j^{(k_0)}(q)}{k_0!} \frac{Q_1^{(k_1)}(q)}{k_1!} \cdots \frac{Q_{N_j}^{(k_m)}(q)}{k_m!}, \ k = 1, 2, \ldots \ .$$

In the case $k < r_{j1} + \cdots + r_{jN_j}$, from $e_j > 1$ and Definition 6.4 it easily follows that for every term of the sum on the right there exists $i \in \{1, \ldots, N_j\}$ such that $k_i = 0$. In other words,

$$k < r_{j1} + \cdots + r_{jN_j} \implies p_j \left| \left(\frac{h^{(k)}(q)}{k!} \right)^{e_j - 1}, \right.$$

from which follows immediately $r_j \geq r_{j1} + \cdots + r_{jN_j} \geq N_j$.

Proof of (8). From Definition 6.4 it can be easily deduced that for each $p \in \Pi$,

$$r_p = 1 \iff p \nmid (h'(q)^{e_p - 1},$$
$$p \nmid (h'(q))^{e_p - 1} \iff \gcd(p^{e_p}, h'(q)) | \mathrm{sqf}(p^{e_p}).$$

Now, since each $r_p \geq 1$, the equivalence follows immediately from the basic equality $\gcd(h(q)/d_h, h'(q)) = \prod_{p \in \Pi} \gcd(p^{e_p}, h'(q))$. □

The following theorem contains our main result about N_f and some of its consequences. For the sake of simplicity and without lost of generality we will limit ourselves to consider primitive polynomials (the general case requires the use of the so-called *primitive part of* $f(X)$, that is, of the primitive polynomial $f_{\mathrm{pr}}(X) := f(X)/\mathrm{c}(f)$).

Theorem 6.6. *Let $f(X)$ be an arbitrary primitive polynomial in $\mathbb{Z}[X]$ of positive degree, and let $(S, \mathcal{Z}, \mathcal{F})$ be any f-admissible triple. Let $(\rho, q, d) \in S \times \mathbb{N}$ such that $d | f(q)$, $q \notin \mathcal{Z}(\rho, q, d)$ and the zeros of $f(X)$ belong to $\mathcal{Z}(\rho, q, d)$. We have*

$$N_f \leq \Delta_{\mathcal{F}(f,\rho,q)}(d) + \sum_{p \in \Pi(f(q)/d)} r_p(f, q). \tag{9}$$

Suppose also that $\gcd(f(q)/d, f'(q)) | \mathrm{sqf}(f(q)/d)$. *Then*

$$N_f \leq \Delta_{\mathcal{F}(f,\rho,q)}(d) + \#(\Pi(f(q)/d)). \tag{10}$$

Moreover,

if $\gcd(f(q), f'(q)) | \mathrm{sqf}(f(q))$, *then* (11)

$$f(X) \text{ is square free and } N_f \leq \Delta^*_{\mathcal{F}(f,\rho,q)}(d) + \#(\Pi(f(q)/d));$$

if $d \leq \mathcal{F}(f, \rho, q)$ *and* $f(q)/d$ *is squarefree, then* (12)

$$f(X) \text{ is square free and } N_f \leq \#(\Pi(f(q)/d)).$$

Proof. Let $\Pi=\Pi(f(q)/d)$ and let $e_p=e_p(f(q)/d)$, $r_p=r_p(f,q)$ for each $p\in\Pi$. Let $g(X)$ be a divisor of $f(X)$ in $\mathbb{Z}[X]$ with the highest possible degree satisfying $g(q)|d$.

Proof of (9). Letting $h(X)=f(X)/g(X)$ and $d_h=d/|g(q)|$ we get at once that $h(X)$ is primitive, $|h(q)|/d_h=|f(q)|/d$ and y $N_f=N_g+N_h$. Therefore, it will be sufficient to prove

$$\text{(i) } N_g\le\Delta_{\mathcal{F}(f,\rho,q)}(d) \text{ and (ii) } N_h\le\sum_{p\in\Pi}r_p.$$

Proof of (i). In case that $g(X)=\pm 1$ we have $N_g=0\le\Delta_{\mathcal{F}(f,\rho,q)}(d)$. Assume that $g(X)$ has positive degree. Therefore we can write $g(X)=g_1(X)\cdots g_{N_g}(X)$, where $N_g\ge 1$ and each $g_j(X)$ is a polynomial in $\mathbb{Z}[X]$ of positive degree that is irreducible in $\mathbb{Z}[X]$. From $g_j(X)|g(X)$ and $g(q)|d$ we obtain $g_j(X)|f(X)$ and $g_j(q)|d$ for $j=1,\dots,N_g$. Hence, since $g(q)|d$, (Condition $\mathcal{A}$) yields

$$|g_j(q)|>\mathcal{F}(f,\rho,q),\ j=1,\dots,N_g,$$

Consequently, as $d=|g_1(q)|\cdots|g_{N_g}(q)|d_h$, (i) follows via Definition 6.2 (a).

Proof of (ii). The given definition of $g(X)$ guarantees that there is no polynomial $k(X)$ in $\mathbb{Z}[X]$ of positive degree with $k(X)|h(X)$ and $k(q)|d_h$. Therefore (ii) follows directly from (7) of Lemma 6.5.

Proof of (10). Considering the case $h(X)=f(X)$, $d_h=d$ of Lemma 6.5, we get from (8) that $\gcd(f(q)/d,f'(q))|\mathrm{sqf}(f(q)/d)$ and $\sum_{p\in\Pi}r_p=\#(\Pi)$ are equivalent statements. Now (10) is an immediate consequence of (9).

Proof of (11). Assume $\gcd(f(q),f'(q))|\mathrm{sqf}(f(q))$. Hence it readily follows

$$\gcd(d,f'(q))|\mathrm{sqf}(d) \text{ and } \gcd(f(q)/d,f'(q))|\mathrm{sqf}(f(q)/d).$$

Therefore, taking into account what has already been proved, it will be sufficient to show that

$$\text{(iii) } f(X) \text{ is square free and (iv) } \gcd(d,f'(q))|\mathrm{sqf}(d) \text{ implies } N_g\le\Delta^*_{\mathcal{F}(f,\rho,q)}(d).$$

Proof of (iii). Suppose that $k_1(X)\in\mathbb{Z}[X]$ satisfies $k_1^2(X)|f(X)$, say $f(X)=k_1^2(X)k_2(X)$ with $k_2(X)\in\mathbb{Z}[X]$. Note first that $|k_1(q)|=1$. Indeed, otherwise there is a prime p dividing $k_1(q)$ and $f'(q)=2k_1'(q)k_1(q)k_2(q)+k_1^2(q)k_2'(q)$, which together with $p^2|f(q)$ contradicts our assumption. From the proof of (ii) above it follows directly that $k_1(X)$ is relatively prime to $h(X)$, so that $k_1(X)|g(X)$. Therefore $k_1(X)$ is a constant polynomial, because otherwise, since $(S,\mathcal{Z},\mathcal{F})$ is f-admissible we would have $1=|k(q)|>\mathcal{F}(f,\rho,q)$ against the definition of $\mathcal{F}$.

Proof of (iv). Suppose that $k_1(X),k_2(X)$ are polynomials in $\mathbb{Z}[X]$ of positive degree with $g(X)=k_1(X)k_2(X)$. From Definition 6.2 (b) and the above proof of (i) we only need to show that $k_1(q)$ and $k_2(q))$ are coprime integers. On the contrary, suppose that a prime p divides $\gcd(k_1(q),k_2(q))$. From $f(X)=g(X)h(X)$ it follows that

$$f'(q)=k_1'(q)k_2(q)h(q)+k_1(q)k_2'(q)h(q)+k_1(q)k_2(q)h'(q),$$

whence we get $p|f'(q)$. Therefore $p|\gcd(d, f'(q))$, which together with $p^2|d$ contradicts $\gcd(d, f'(q))|\mathrm{sqf}(d)$.

Proof of (12). Assume $d \le \mathcal{F}(f,\rho,q)$ and that $f(q)/d$ is square free. These assumptions guarantee $\Delta_{\mathcal{F}(f,\rho,q)}(d)=0$ and $\gcd(f(q)/d, f'|\mathrm{sqf}(f(q)/d)$ respectively, so (10) yields $N_f \le \#(\Pi)$. In order to prove that $f(X)$ is square free suppose that $k(X)$ is a polynomial in $\mathbb{Z}[X]$ satisfying $k^2(X)|f(X)$. Certainly we can write $k(q) = ab$, with $a|d$ and $b|(f(q)/d)$. Since $k^2(q) = a^2b^2$ and $f(q)/d$ is square free, we have $ab|d$, that is, $k(q)|d$. Therefore $k(X)$ is a constant polynomial, because otherwise, as $(S,\mathcal{Z},\mathcal{F})$ is f-admissible we would have $|k(q)| > \mathcal{F}(f,\rho,q)$ against $d \le \mathcal{F}(f,\rho,q)$. □

At this point it can be readily seen that the case $f(X)$ primitive of positive degree of Theorem 2.2 is equivalent to the case $\Delta_{\mathcal{F}(f,\rho,q)}(d) = 0$, $\#(\Pi(f(q)/d) = 1$ of (10). Furthermore, replacing here the hypothesis $\gcd(f(q)/d,f'(q))|\mathrm{sqf}(f(q)/d)$ by $\delta(|f(q)|,|f'(q)|)|d$ (see Definition 2.3) we get a direct generalization of Corollary 2.4. Consequently, the case $d = |f(q)|$ of Theorem 6.6 yields (see Remark 6.3)

$$(9^*)\, N_f \le \Delta_{\mathcal{F}(f,\rho,q)}(|f(q)|) \text{ and } (11^*)\, N_f \le \Delta^*_{\mathcal{F}(f,\rho,q)}(|f(q)|),$$

which in general improve the estimations for N_f established in (9) and (11). It is also clear that (12) generalizes the case $e = 1$ of Theorem 2.2. As an application we will prove the following extension of Filaseta's Theorem 2.

Corollary 6.7. *Let t be a positive integer and let $p_1, \ldots, p_t$ be distinct prime numbers. Let q, a be positive integers with $ap_1\cdots p_t \ge q > a$. Let $f(X)$ denote the polynomial in $\mathbb{Z}[X]$ which is obtained replacing q by X in the representation of $ap_1\cdots p_t$ in base q. Then*

$$f(X) \text{ is squarefree and } N_f \le t. \tag{13}$$

Proof. Let $d = a/\gcd(a, \mathrm{c}(f))$. As $f(X)$ has nonnegative coefficients the hypothesis $ap_1\cdots p_t \ge q > a \ge d$ ensures that $f(X)$ has positive degree and $f(q-d) \ne 0$. Hence, from Lemma 4.6, we can use in Theorem 6.6 the triple $(S,\mathcal{Z},\mathcal{F})_{v=1}^{\mathrm{P\&S}}$ with $\rho = \sqrt{q}$. Note also that $q - 1 < 2(q - \sqrt{q})$, so that $d \le a \le q - 1 < 2(q - \sqrt{q}) = \mathcal{F}(f,\rho,q)$.

At this point it should be noticed that the aforementioned properties of $f(X)$ are also satisfied by $f_{\mathrm{pr}}(X) = f(X)/\mathrm{c}(f)$, the primitive part of $f(X)$. Furthermore, since $c = \mathrm{c}(f)/\gcd(a, \mathrm{c}(f))$ is relatively prime to a and therefore to d, we have that c divides $p_1\cdots p_t$ from which it follows $f_{\mathrm{pr}}(q) = ap_1\cdots p_t/\mathrm{c}(f) = d(p_1\cdots p_t/c)$, which ensures that $f_{\mathrm{pr}}(q)/d$ is square free. Thus, since all the conditions required in Theorem 6.6 to prove (12) are satisfied with $f_{\mathrm{pr}}(X)$ instead of $f(X)$, and the equality above also implies $\#(\Pi(f_{\mathrm{pr}}(q))/d) \le t$, we get that $f_{\mathrm{pr}}(X)$ is square free and $N_{f_{\mathrm{pr}}} \le t$. Hence, as $N_f = N_{f_{\mathrm{pr}}}$ and $f(X)$ is square free if and only if $f_{\mathrm{pr}}(X)$ is, the proof of (13) is complete. □

References

[1] P. T. Bateman and R. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math Comp. **16** (1962), 363-367.

[2] J. Brillhart, *Note on irreducibility testing*, Math. Comp. **35**, (1980) 1379–1381.

[3] J. Brillhart, M. Filaseta M. and A. Odlizko, *On an irreducibility theorem of A. Cohn*, Canadian J. Math. **5** (1981), 1055–1059.

[4] Y. Chen, G. Kun, G. Pete and I. Z. Ruzsa, *Prime values of reducible polynomials, II*, Acta Arithmetica **104** (2002), no. 2, 117–127.

[5] L. E. Dickson, History of the Theory of Numbers, Vol 1, Chelsea, 1971, 332–334.

[6] H. L. Dorwarth, *Irreducibility of polynomials*, Amer. Math. Monthly **42** (1935), no. 6, 369–381.

[7] M. Filaseta, *A Further generalization of an irreducibility theorem of A. Cohn*, Canadian J. Math. **6**, (1982), 1390–1395.

[8] M. Filaseta, *Irreducibility criteria for polynomials with non-negative coefficients*, Canadian J. Math. **XV**, (1988), 339–351.

[9] K. Girstmair, *On an irreducibility criterion of M. Ram Murty*, Amer. Math. Monthly **112** (2005), 269–270.

[10] N. H. Guersenzvaig and F. Szechtman, *Roots multiplicity and square free factorization of polynomials using companion matrices*, Linear algebra and its Applications **436** (2012), 3160–3164.

[11] M. Marden, The Geometry of the Zeros of a Polynomial in a Complex Variable, AMS, 1949, p. 96.

[12] K. S. McCurley, *Prime values of polynomials and irreducibility testing*, Bull. Amer. Math. Society **11** (1984), 155–158.

[13] M. Mignotte and D. Stefanescu, Polynomials. An Algorithmic approach, Springer (1999), 22–23, 58–63.

[14] O. Ore, *Einige Bemerkungen über Irreduzibilität*, Jahresbericht der Deutschen Mathematiker-Vereinigung **44** (1934), 147–151.

[15] G. Pólya und G. Szegö, Aufgaben und Lehrsätze aus der Analysis II, Springer-Verlag, 1925, 137, 350–351.

[16] G. Pólya and G. Szegö, Problems and Theorems in Analysis I, Springer-Verlag, 1976, 107, 301.

[17] G. Pólya and G. Szegö, Problems and Theorems in Analysis II, Springer-Verlag, 1976, 130, 133, 330.

[18] V. V. Prasolov, Polynomials, Springer, 2004, pp. 47–74.

[19] M. Ram Murty, *Prime numbers and irreducible polynomials*, Amer. Math. Monthly **109** (2002), 452-458.

[20] P. Stäckel, *Arithmetischen Eigenschaften ganzer Funktionen*, Journal für Mathemathik **148** (1918), 101–112.

[21] L. Weisner, *Criteria for the irreducibility of polynomials*, Bulletin of the Amer. Math. Society **40** (1934), 864–870.

Appendix A

Here we prove Lemma 4.6. A straightforward calculation shows that $\sqrt{3}(1+\sqrt{4m+1})/4 \le \sqrt{m+1}$ for any positive integer m (equality holds if and only if $m=2$). Thus Lemma 4.6 is an immediate consequence of the case $M \le q-1$ of the result below.

Lemma 4.6*. *Let $f(X)=\sum_{k=0}^{n} a_k X^k \in \mathbb{C}[X]$, $\Re(a_n) \ge 1$ and $\Re(a_{n-k}) \ge 0$ for $k=1,2,3$. Let $M=\max_{k=0,1,\ldots,n-2} |a_k/\Re(a_n)|$. Then the zeros of $f(X)$ lie in the half plane*

$$\Re(z) < \frac{\sqrt{3}(1+\sqrt{4M+1})}{4}.$$

Proof. Let w be any complex number with $|w|>1$. For $k=1,\ldots,n$ we have,

$$\begin{aligned}\left|\frac{f(w)}{w^n}\right| &\ge \left|a_n+\frac{a_{n-1}}{w}+\cdots+\frac{a_{n-k}}{w^k}\right| - \frac{|a_{n-k-1}|}{|w|^{k+1}} - \cdots - \frac{|a_0|}{|w|^n} \\ &> \Re\left(a_n+\frac{a_{n-1}}{w}+\cdots+\frac{a_{n-k}}{w^k}\right) - \frac{M\Re(a_n)}{|w|^{k+1}-|w|^k}. \end{aligned} \tag{14}$$

Now we assume $\Re(w)>0$. Certainly

$$\Re\left(\frac{1}{w}\right) = \frac{\Re(w)}{|w|} > 0. \tag{15}$$

Hence, letting $k=1$ in (14), from $\Re(a_n)\ge 1$ and $\Re(a_{n-1})\ge 0$ we get,

$$\begin{aligned}&\left|\frac{|w|^2-|w|}{w^n}\right| |f(w)| > |w|^2-|w|-M) \\ &\qquad = \left(|w| - \frac{1+\sqrt{4M+1}}{2}\right)\left(|w| - \frac{1-\sqrt{4M+1}}{2}\right).\end{aligned}$$

In this way we arrive to a well-known fact, namely, the roots of $f(X)$ with positive real part are in the disk

$$|w| < \frac{1+\sqrt{4M+1}}{2}. \tag{16}$$

Now assume $\Re(w) \ge B(M)$, where $B(M)=\sqrt{3}(1+\sqrt{4M+1})/4$. From (16) we obtain

$$\cos(\arg(w)) = \frac{\Re(w)}{|w|} > \frac{B(M)}{\frac{1+\sqrt{4M+1}}{2}} = \frac{\sqrt{3}}{2}.$$

Consequently, $\arg(w) < \pi/6$, whence $\Re(1/w^k) = \cos(k\arg(w))/|w|^k > 0$ for $k=2,3$. Thus, letting $k=3$ in (14), from (15), $\Re(a_{n-2})\ge 0$ and $\Re(a_{n-3})\ge 0$ we get

$$\left|\frac{|w|^4-|w|^3}{w^n}\right| |f(w)| > |w|^4-|w|^3-M.$$

The function h defined over $\mathbb{R}$ by $h(x) = x^4 - x^3 - M$ is strictly increasing in the interval $(3/4, +\infty)$. On the other hand, it can be readily verified that $-M = -4B^2(M)/3 + 4B(M)/\sqrt{3}$. Then, since $|w| \geq B(M) \geq \sqrt{3}/2 > 3/4$ and $3X^3 - 3X^2 - 4X + 4\sqrt{3}$ has no positive real zeros, we have

$$\left|\frac{|w|^4 - |w|^3}{w^n}\right| |f(w)| > h(|w|) \geq h(B(M)) = B^4(M) - B^3(M) - M$$
$$= B(M)(3B^3(M) - 3B^2(M) - 4B(M) + 4\sqrt{3})/3 > 0$$
$$> 0.$$

Hence, as $f(w) \neq 0$ for $\Re(w) \geq B(M)$, the proof is complete. □

Appendix B

Here we shall prove Theorem 4.7.

Proof. Let $(b_m \dots b_1 b_0)_{(q)}$ denote the base q representation of $b = dp^e$ (with $b_m \neq 0$), which means (as usual $[x]$ stands for the integer part of any real number x)

$$b = \sum_{0 \leq k \leq m} b_k q^k, \text{ with } b_k = [b/q^k] - q[b/q^{k+1}] \text{ for } k = 0, 1, \dots, m = [\log b / \log q].$$

Obviously, we have $f(q) = dp^e$. Our assumption $d < q < dp^e$ guarantees that $f(X)$ has positive degree and $f(q-d) \neq 0$. On the other hand, Lemma 4.6 ensures that the zeros of $f(X)$ are in the half plane $\Re(z) < \sqrt{q}$. Now, since $q > \sqrt{q} + \frac{1}{2}$, from (2^*) of the case $\rho = \sqrt{q}$ of Theorem 4.4 it follows immediately that for proving that $f(X)$ is irreducible in $\mathbb{Q}[X]$ only remains to show that $p \nmid (f'(q))^{e-1}$. To this end, note first that from the above definition of $f(X)$ and $q = pa$ are easily deduced the following equivalences:

$$p \nmid f'(q) \iff p \nmid [dp^{e-1}/a] \iff p \nmid b_1. \tag{17}$$

Proof of (4). It can be readily shown that for arbitrary positive integers n, k and j, with $k, j \in \{1, \dots, n\}$,

$$[n/k] = j \iff n/(j+1) < k \leq n/j.$$

Replacing n, k and j by dp^e, q and jp, respectively, for the case $e > 1$ we obtain

$$[dp^e/q] = jp \iff dp^e/(jp+1) < q \leq dp^e/jp \text{ for } j = 1, 2, \dots, dp^{e-1}.$$

Equivalently, we can write

$$p \nmid [dp^e/q] \iff q \notin \bigcup_{1 \leq j < dp^{e-1}} \left(\frac{dp^e}{pj+1}, \frac{dp^e}{pj}\right],$$

which togheter with the first equivalence of (17) completes the proof of (4).

From now on r denotes the remainder of dividing d by a.

Proof of (5). Suppose that $a^2|(p-1)$ and $r \neq 0$. From (17) it follows that we only need to show that $p \nmid b_1^{e-1}$, so here we also assume $e \geq 2$. First we will prove, inductively, that there is a positive integer n such that the base q representation of p^e has the form $p^e = (c_n \dots c_0)_{(q)}$ with $(c_1, c_0) = (a^*, p)$, where $a^* = (p-1)/a$.

When $e = 2$ we have $p^2 = p(aa^* + 1) = a^*pa + p = (a^*p)_{(q)}$. Now suppose $2 \leq i < e$ and $p^i = (c_n \dots c_0)_{(q)}$ with $(c_1, c_0) = (a^*, p)$. Therefore, since $p^{i+1} \equiv p(a^*q + p) \pmod{q^2}$, we just need to prove that the representation of $p(a^*q+p)$ in base q has the form $(sa^*p)_{(q)}$. From $a^2|(p-1)$ we get $a^* = sa$ with $s = (p-1)/a^2 < q$, so $p(a^*q + p) = s(pa)^2 + p^2 = s(pa)^2 + a^*(pa) + p$, as we wanted to show.

Therefore, assuming that the base q representation of p^e has the form $p^e = (c_n \dots c_0)_{(q)}$ with $(c_1, c_0) = (a^*, p)$, we have $dp^e \equiv d(a^*q + p) \pmod{q^2}$. As before we only need to consider the representation of $d(a^*q + p)$ in base q. Let $j = [d/a]$. From $d = ja + r$ we get

$$\begin{aligned} d(a^*q + p) &= da^*q + dp = da^*q + jq + rp \\ &= (da^* + j)q + rp = (jaa^* + ra^* + j)q + rp \\ &= (jp + ra^*)q + rp. \end{aligned}$$

Notice that $jp + ra^* = (pd - r)/a < pd/a < p^2 < q^2$. Consequently, there are integers s_1, s_2 in the interval $[0, q)$ such that

$$jp + ra^* = s_2q + s_1.$$

From $0 < r < a$, $a|a^*$ and $a^* < p$ it follows that both a^* and r are relatively prime to p. Then $p \nmid s_1$, because otherwise we have the contradiction $p|ra^*$. Finally, since $rp < q$, the equality

$$d(a^*q + p) = s_2q^2 + s_1q + rp$$

yields $b_0 = rp$, and hence $s_1 = b_1$ as we needed to show.

Proof of (6). Assume that $a^2|(p-1)$ and $\gcd(d, [d/a]q) = 1$. From $a \geq 2$ and

$$\gcd(d, rp) = \gcd(d, (d-r)p) = \gcd(d, [d/a]q) = 1 \tag{18}$$

it easily follows $r \neq 0$, so the previous proof and (17) guarantee that $p \nmid (f'(q))^{e-1}$. We have also proved above that $b_0 = rp$ when $e \geq 2$. Since $dp = [d/a]q + rp$, such equality holds as well for $e = 1$. Thus, since (18) implies $\gcd(d, \mathrm{c}(f)) = 1$, in accordance with (3^*) of Theorem 4.4 we can conclude that $f(X)$ is irreducible in $\mathbb{Z}[X]$. □