Apollonius circles and the number of irreducible factors of polynomials

by

Anca Iuliana Bonciocat[1], Nicolae Ciprian Bonciocat[2], Yann Bugeaud[3],
Mihai Cipu[4], Maurice Mignotte[5]

Dedicated to Professors Toma Albu and Constantin Năstăsescu
on the occasion of their 80th birthdays

Abstract

We provide upper bounds for the sum of the multiplicities of the non-constant irreducible factors that appear in the canonical decomposition of a polynomial $f(X) \in \mathbb{Z}[X]$, in case all the roots of f lie inside an Apollonius circle associated to two points on the real axis with integer abscissae a and b, with ratio of the distances to these points depending on the admissible divisors of $f(a)$ and $f(b)$. In particular, we obtain such upper bounds for the case where $f(a)$ and $f(b)$ have few prime factors, and f is an Eneström-Kakeya polynomial, or a Littlewood polynomial, or has a large leading coefficient. Similar results are also obtained for multivariate polynomials over arbitrary fields, in a non-Archimedean setting.

Key Words: Apollonius circles, irreducible polynomial, prime number.
2020 Mathematics Subject Classification: Primary 11R09; Secondary 11C08.

1 Introduction

The prime factorization of the values that an integer polynomial $f(X)$ takes at some specified integral arguments gives useful information on the canonical decomposition of f. Many of the classical or more recent irreducibility criteria make use of such information, combined with information on the location of the roots of f. One may find such classical results in the works of Stäckel [28], Weisner [29], Ore [24] and Dorwart [14]. For more recent results and some elegant connections between prime numbers and irreducible polynomials we refer the reader to Ram Murty [27], Girstmair [18], Guersenzvaig [19], and Bodin, Dèbes and Najib [3], for instance. Some particularly elegant irreducibility criteria write prime numbers or some classes of composite numbers in the number system with base B, say, and then replace the base by an indeterminate to produce irreducible polynomials. Here we mention Cohn's irreducibility criterion [26] that uses prime numbers written in the decimal system, and its generalization by Brillhart, Filaseta and Odlyzko [8] to an arbitrary base, as well as further generalizations by Filaseta [15], [16], and by Cole, Dunn and Filaseta [11]. Another way to produce irreducible polynomials f is to write prime numbers or prime powers as sums of integers of arbitrary sign, one of these integers having a sufficiently large absolute value, and to use these integers as coefficients of f [4], [6].

In [5] the irreducibility of an integer polynomial f was studied by combining information on the *admissible divisors* of $f(a)$ and $f(b)$ for two integers a and b, with information on the location of the roots of f. We recall here the definition of admissible divisors, that will be also required throughout this paper.

Definition 1. *Let f be a non-constant polynomial with integer coefficients, and let a be an integer with $f(a) \neq 0$. We say that an integer d is an admissible divisor of $f(a)$ if $d \mid f(a)$ and*

$$\gcd\left(d, \frac{f(a)}{d}\right) \mid \gcd(f(a), f'(a)), \tag{1.1}$$

and we shall denote by $\mathcal{D}_{ad}(f(a))$ the set of all admissible divisors of $f(a)$. We say that an integer d is a unitary divisor of $f(a)$ if $d \mid f(a)$ and d is coprime with $f(a)/d$. We denote by $\mathcal{D}_u(f(a))$ the set of unitary divisors of $f(a)$.

We note that this definition was motivated by the fact that if a polynomial $f(X) \in \mathbb{Z}[X]$ factors as $f(X) = g(X)h(X)$ with g, h non-constant polynomials in $\mathbb{Z}[X]$, then given an integer a with $f(a) \neq 0$, the integers $g(a)$ and $h(a)$ are divisors of $f(a)$ which must also satisfy the equality $f'(a) = g'(a)h(a) + g(a)h'(a)$. This implies that the greatest common divisor of $g(a)$ and $\frac{f(a)}{g(a)}$ must divide both $f(a)$ and $f'(a)$. We also note that if $f(a)$ and $f'(a)$ are coprime, then $\mathcal{D}_{ad}(f(a))$ reduces to the set $\mathcal{D}_u(f(a))$.

As seen in [5], one can connect the study of the irreducibility of f with the location of the roots of f inside an Apollonius circle associated to the points on the real axis with integer abscissae a and b, and ratio of the distances to these two points expressed only in terms of some admissible divisors of $f(a)$ and $f(b)$. We recall here the famous definition of a circle given by Apollonius, as the set of points P in the plane that have a given ratio r of distances to two fixed points A and B (see Figure 1), which may degenerate to a point (for $r \to 0$ or $r \to \infty$) or to a line (for $r \to 1$).
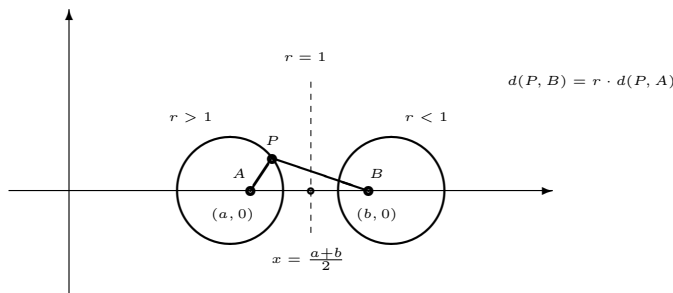

Figure 1. The Apollonius circles associated to a pair of points in the plane

More precisely, given two points $A = (a, 0)$ and $B = (b, 0)$ and $r > 0$, $r \neq 1$, the set of points $P = (x, y)$ with $d(P, B) = r \cdot d(P, A)$ is the Apollonius circle $\mathrm{Ap}(a, b, r)$ given by the equation

$$\left(x - \frac{ar^2 - b}{r^2 - 1}\right)^2 + y^2 = \left(r\frac{b - a}{r^2 - 1}\right)^2, \tag{1.2}$$

which degenerates to the point $(b, 0)$ for $r \to 0$, to the point $(a, 0)$ for $r \to \infty$, and to the vertical line $x = \frac{a+b}{2}$ for $r \to 1$.

Consider the canonical decomposition $f(X) = const \cdot \prod_{i=1}^{r} f_i(X)^{m_i}$ of a polynomial $f \in \mathbb{Z}[X]$, with the f_i's irreducible and prime to each other. The aim of this paper is to generalize the results in [5] by obtaining upper bounds for $m_1 + \cdots + m_r$. This will be achieved by adapting the methods in [5] and considering a sequence of potentially larger Apollonius circles that might contain the roots of f, and here too, the admissible divisors of $f(a)$ and $f(b)$ will play a crucial role. For other results that bound the sum of these multiplicities we refer the reader to Guersenzvaig [19], and to [7], where some methods of Cavachi, M. Vâjâitu and Zaharescu [9], [10] to study linear combinations of relatively prime polynomials have been employed.

Throughout the paper, instead of saying that the sum of the multiplicities of the non-constant irreducible factors that appear in the canonical decomposition of f is at most k, we will simply say that f is the product of at most k irreducible factors over $\mathbb{Q}$.

Our first result that establishes a connection between Apollonius circles and the sum of these multiplicities is the following.

Theorem 1. *Let $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$, and assume that for two integers a, b we have $0 < |f(a)| < |f(b)|$. Let k be a positive integer, and let*

$$q_k = \max \left\{ \frac{d_2}{d_1} \leq \sqrt[k+1]{\frac{|f(b)|}{|f(a)|}} : d_1 \in \mathcal{D}_{ad}(f(a)), \ d_2 \in \mathcal{D}_{ad}(f(b)) \right\}. \tag{1.3}$$

Then f is the product of at most k irreducible factors over $\mathbb{Q}$ in each one of the following three cases:

i) $q_k > 1$ *and all the roots of f lie inside the Apollonius circle $\mathrm{Ap}(a, b, q_k)$;*

ii) $q_k > 1$, *all the roots of f lie inside the Apollonius circle $\mathrm{Ap}(a, b, \sqrt{q_k})$, and f has no rational roots;*

iii) $q_k = 1$ *and either $b > a$ and all the roots of f lie in the half-plane $x < \frac{a+b}{2}$, or $a > b$ and all the roots of f lie in the half-plane $x > \frac{a+b}{2}$.*

We mention that by taking $k = 1$ in Theorem 1, we recover Theorem 1 in [5]. Theorem 1 can be given in a more explicit form by taking into account the equation of the Apollonius circles given by (1.2), as follows.

Theorem 2. *Let $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$, and assume that for two integers a, b we have $0 < |f(a)| < |f(b)|$. Let k be a positive integer and let q_k be given by (1.3). Then f is the product of at most k irreducible factors over $\mathbb{Q}$ in each one of the following three cases:*

i) $q_k > 1$ *and each root θ of f satisfies $|\theta - \frac{aq_k^2 - b}{q_k^2 - 1}| < q_k \frac{|b - a|}{q_k^2 - 1}$;*

ii) $q_k > 1$, *each root θ of f satisfies $|\theta - \frac{aq_k - b}{q_k - 1}| < \sqrt{q_k} \frac{|b - a|}{q_k - 1}$, and f has no rational roots;*

iii) $q_k = 1$ *and either $b > a$ and all the roots of f lie in the half-plane $x < \frac{a+b}{2}$, or $a > b$ and all the roots of f lie in the half-plane $x > \frac{a+b}{2}$.*

Notice that if $b > a$ and we can prove that $q_k = 1$ for some $k \geq 1$, by imposing the condition that $f(X + \frac{a+b}{2})$ is a Hurwitz stable polynomial, so that all the roots of f lie in

the half-plane $x < \frac{a+b}{2}$, then by Theorem 1 iii) we may conclude that f is the product of at most k irreducible factors over $\mathbb{Q}$. Recall that a necessary and sufficient condition for a polynomial to be Hurwitz stable is that it passes the Routh–Hurwitz test.

In some situations, instead of testing the conditions in Theorem 1 or Theorem 2, it might be more convenient to use the maximum of the absolute values of the roots of f:

Theorem 3. *Let $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$, let M be the maximum of the absolute values of its roots, and assume that for two integers a, b we have $0 < |f(a)| < |f(b)|$. Let k be a positive integer and let q_k be given by (1.3). Then f is the product of at most k irreducible factors over $\mathbb{Q}$ in each one of the following three cases:*

   i) $|b| > q_k|a| + (1 + q_k)M$;
   ii) $|b| > \sqrt{q_k}|a| + (1 + \sqrt{q_k})M$ *and f has no rational roots;*
   iii) $q_k = 1$, $a^2 < b^2$ *and* $M < \frac{|a+b|}{2}$.

As we shall see later in Remark 1, in some cases, conditions i) and ii) in Theorem 2 may lead to sharper conditions than the corresponding ones in Theorem 3, even if we don't explicitly compute the coefficients of $f(X + \frac{aq_k^2 - b}{q_k^2 - 1})$ and $f(X + \frac{aq_k - b}{q_k - 1})$ to derive then estimates for the maximum of the absolute values of their roots. However, by computing these coefficients and avoiding unnecessary use of the triangle inequality, one might obtain even sharper conditions on a and b.

When there is no information available on the prime factorization of $f'(a)$ and $f'(b)$, thus preventing one to use the admissible divisors of $f(a)$ and $f(b)$, we may content ourselves with slightly weaker results by allowing d_1 and d_2 in the definition of q_k to be arbitrary divisors of $f(a)$ and $f(b)$, respectively. This will potentially increase q_k, leading to stronger restrictions on a and b. The computation of q_k requires analyzing inequalities between products of prime powers, so an explicit, effective formula of q_k can be obtained only in a few cases where $f(a)$ and $f(b)$ have a small number of prime factors. On the other hand, one may relax the restrictions on a and b by finding sharp estimates for M, the maximum of the absolute values of the roots of f. The reader may benefit of the extensive literature on this subject, originating in the works of Cauchy and Lagrange. Here we will only refer the reader to the generalization for Cauchy's bound on the largest root of a polynomial [23], to a recent improvement of the bound of Lagrange [2], to some classical results relying on families of parameters obtained by Fujiwara [17], Ballieu [1], [22], Cowling and Thron [12], [13], Kojima [21], and to methods that use estimates for the characteristic roots for complex matrices [25].

The results stated so far will be proved in Section 2. We will present in Section 3 some corollaries of Theorem 3, for some cases where the prime factorizations of $f(a)$ and $f(b)$ allow one to conclude that $q_k = 1$. Results that rely on information on the unitary divisors of $f(a)$ and $f(b)$ will be given in Section 4. In Section 5 we will provide some analogous results for multivariate polynomials over arbitrary fields. Some examples will be given in the last section of the paper.

2   Proofs for the case of admissible divisors

Proof of Theorem 1 First of all let us notice that, if we fix the integers a and b as in the statement of the theorem, then q_k is a decreasing function on k. Moreover, since 1 is

obviously an admissible divisor of $f(a)$ and $f(b)$, a possible candidate for q_k is 1, so $q_k \geq 1$ for each k. Assume now to the contrary that f is the product of s factors $f_1, \ldots, f_s \in \mathbb{Z}[X]$ with $s \geq k+1$ and $f_1, \ldots, f_s$ irreducible over $\mathbb{Q}$. Next, let us select an index $i \in \{1, \ldots, s\}$ and let us denote

$$g_i(X) := \prod_{j \neq i} f_j(X).$$

We may thus write $f = f_i \cdot g_i$ for each $i = 1, \ldots, s$. Now, since $f(a) = f_i(a)g_i(a) \neq 0$ and $f'(a) = f_i'(a)g_i(a) + f_i(a)g_i'(a)$, and similarly $f(b) = f_i(b)g_i(b) \neq 0$ and $f'(b) = f_i'(b)g_i(b) + f_i(b)g_i'(b)$, we see that $f_i(a)$ is a divisor d_i of $f(a)$, and $f_i(b)$ is a divisor d_i' of $f(b)$ that must also satisfy the following divisibility conditions

$$\gcd\left(d_i, \frac{f(a)}{d_i}\right) \mid \gcd(f(a), f'(a)) \quad \text{and} \quad \gcd\left(d_i', \frac{f(b)}{d_i'}\right) \mid \gcd(f(b), f'(b)).$$

Therefore d_i and d_i' are admissible divisors of $f(a)$ and $f(b)$, respectively, and this holds for each $i = 1, \ldots, s$. Next, since

$$\frac{d_1'}{d_1} \cdots \frac{d_s'}{d_s} = \frac{f(b)}{f(a)},$$

one of the quotients $\frac{|d_1'|}{|d_1|}, \ldots, \frac{|d_s'|}{|d_s|}$, say $\frac{|d_1'|}{|d_1|}$, must be less than or equal to $\sqrt[s]{\frac{|f(b)|}{|f(a)|}}$. In particular, this shows that we must have

$$\frac{|f_1(b)|}{|f_1(a)|} \leq q_{s-1}. \tag{2.1}$$

Assume now that f factors as $f(X) = a_n(X - \theta_1) \cdots (X - \theta_n)$ for some complex numbers $\theta_1, \ldots, \theta_n$. Without loss of generality we may further assume that $\deg f_1 = m \geq 1$, say, and that

$$f_1(X) = b_m(X - \theta_1) \cdots (X - \theta_m)$$

for some divisor b_m of a_n. Next, we observe that we may write

$$\frac{f_1(b)}{f_1(a)} = \frac{b - \theta_1}{a - \theta_1} \cdots \frac{b - \theta_m}{a - \theta_m},$$

so in view of (2.1) for at least one index $j \in \{1, \ldots, m\}$ we must have

$$\frac{|b - \theta_j|}{|a - \theta_j|} \leq q_{s-1}^{\frac{1}{m}}. \tag{2.2}$$

Now, let us first assume that $q_k > 1$ and all the roots of f lie inside the Apollonius circle $\mathrm{Ap}(a, b, q_k)$. In particular, since θ_j lies inside the Apollonius circle $\mathrm{Ap}(a, b, q_k)$, it must satisfy the inequality $|b - \theta_j| > q_k|a - \theta_j|$. Since $q_k > 1$ and $m \geq 1$, we have $q_k \geq q_k^{\frac{1}{m}}$, so we deduce that we actually have

$$\frac{|b - \theta_j|}{|a - \theta_j|} > q_k^{\frac{1}{m}} \geq q_{s-1}^{\frac{1}{m}},$$

as $q_k \geq q_{s-1}$, and this contradicts (2.2). Therefore f is the product of at most k irreducible factors over $\mathbb{Q}$.

Next, assume that $q_k > 1$ and that all the roots of f lie inside the Apollonius circle $\mathrm{Ap}(a, b, \sqrt{q_k})$. In particular, we have $|b - \theta_j| > \sqrt{q_k}|a - \theta_j|$. Since f has no rational roots, we must have $m \geq 2$, so $\sqrt{q_k} \geq q_k^{\frac{1}{m}}$, which also leads us to the desired contradiction

$$\frac{|b - \theta_j|}{|a - \theta_j|} > q_k^{\frac{1}{m}} \geq q_{s-1}^{\frac{1}{m}},$$

so in this case too one may write f as a product of at most k irreducible factors over $\mathbb{Q}$.

Finally, let us assume that $q_k = 1$. Since $1 \leq q_{s-1} \leq q_k$, this implies that q_{s-1} is also equal to 1, so in this case inequality (2.2) reads

$$\frac{|b - \theta_j|}{|a - \theta_j|} \leq 1,$$

which is equivalent to

$$(b - Re(\theta_j))^2 \leq (a - Re(\theta_j))^2. \tag{2.3}$$

To contradict (2.3), it is therefore sufficient to ask all the roots of f to lie in the half-plane $x < \frac{a+b}{2}$ if $a < b$, or in the half-plane $x > \frac{a+b}{2}$ if $a > b$, and this completes the proof.   □

Proof of Theorem 2 i) In view of (1.2), the abscissa of the center of the Apllonius circle $\mathrm{Ap}(a, b, q_k)$ is $C_k = \frac{aq_k^2 - b}{q_k^2 - 1}$, and its radius is $R_k = q_k \frac{|b-a|}{q_k^2 - 1}$. The condition that all the roots of f lie inside the Apollonius circle $\mathrm{Ap}(a, b, q_k)$ is equivalent to asking all the roots of the polynomial $f(X + C_k)$ to lie inside the circle centered in the origin and with radius R_k, or equivalenly, that all the roots of $f(X + C_k)$ have absolute values less than R_k. Thus, if the roots of f are $\theta_1, \ldots, \theta_n$, say, then the roots of $f(X + C_k)$ are $\theta_1 - C_k, \ldots, \theta_n - C_k$, and our condition on $\theta_1, \ldots, \theta_n$ reads

$$\max_{1 \leq i \leq n} |\theta_i - C_k| < R_k. \tag{2.4}$$

ii) Here the abscissa of the center of the Apllonius circle $\mathrm{Ap}(a, b, \sqrt{q_k})$ is $C_k' = \frac{aq_k - b}{q_k - 1}$, and its radius is $R_k' = \sqrt{q_k} \frac{|b-a|}{q_k - 1}$. One argues as in the previous case with C_k' instead of C_k and R_k' instead of R_k.   □

Remark 1. *We mention that, using the notation in the proof of Theorem 2, we have*

$$f(X + C_k) = \sum_{i=0}^{n} b_i X^i \quad \text{with} \quad b_i = \sum_{j=i}^{n} a_j \binom{j}{i} C_k^{j-i}, \tag{2.5}$$

so when it is possible, to test (2.4) one should compute the coefficients b_i in (2.5) and then apply some known estimates for the roots of $f(X + C_k)$ in terms of the b_i's. When the computation of the b_i's is rather difficult, one may use a condition stronger than (2.4), that is

$$\max_{1 \leq i \leq n} |\theta_i| < R_k - |C_k|,$$

provided $R_k > |C_k|$, or equivalently, that $q_k|b - a| > |aq_k^2 - b|$. In this way one may directly use some suitable estimates for $M := \max_{1 \leq i \leq n} |\theta_i|$ in terms of the coefficients of f, thus avoiding the computation of the b_i's, and in some cases the outcome may consist of

sharper conditions on a and b than those in Theorem 3 i). To see this, we will assume that $q_k > 1$ and we will present the cases where $R_k > |C_k|$, depending on the signs of a and b and on their magnitude:

1) If $a > 0 > b$, $|b| > a$ and $q_k < \frac{|b|}{a}$, then $R_k - |C_k| = -\frac{aq_k+b}{q_k+1} > 0$, and our condition $M < R_k - |C_k|$ leads us to $|b| > q_k|a| + (1 + q_k)M$;

2) If $b > a > 0$ and $q_k < \sqrt{\frac{b}{a}}$, then $R_k - |C_k| = \frac{aq_k+b}{q_k+1} > 0$, and condition $M < R_k - |C_k|$ leads to $|b| > -q_k|a| + (1 + q_k)M$;

3) If $b > a > 0$ and $\sqrt{\frac{b}{a}} \le q_k < \frac{b}{a}$, then $R_k - |C_k| = \frac{-aq_k+b}{q_k-1} > 0$, and condition $M < R_k - |C_k|$ leads to $|b| > q_k|a| + (q_k - 1)M$;

4) If $a = 0$ and $b \neq 0$, then $R_k - |C_k| = \frac{|b|}{q_k+1} > 0$, and condition $M < R_k - |C_k|$ leads to $|b| > (1 + q_k)M$;

5) If $a < 0 < b$, $b > |a|$ and $q_k < \frac{b}{|a|}$, then $R_k - |C_k| = \frac{aq_k+b}{q_k+1} > 0$, and condition $M < R_k - |C_k|$ leads to $|b| > q_k|a| + (1 + q_k)M$;

6) If $b < a < 0$ and $q_k < \sqrt{\frac{b}{a}}$, then $R_k - |C_k| = -\frac{aq_k+b}{q_k+1} > 0$, and our condition $M < R_k - |C_k|$ leads to $|b| > -q_k|a| + (1 + q_k)M$;

7) If $b < a < 0$ and $\sqrt{\frac{b}{a}} \le q_k < \frac{b}{a}$, then $R_k - |C_k| = \frac{aq_k-b}{q_k-1} > 0$, and condition $M < R_k - |C_k|$ leads to $|b| > q_k|a| + (q_k - 1)M$.

Thus, in cases 2), 3) and 6), 7) we reach the same conclusion as in Theorem 3 i), but with a less restrictive condition than $|b| > q_k|a| + (1 + q_k)M$.

Similar considerations apply to case ii) of Theorem 3 as well.

Proof of Theorem 3 The proof follows the same lines as in the case of Theorem 1, and we deduce again that for at least one index $j \in \{1, \ldots, m\}$ we must have

$$\frac{|b - \theta_j|}{|a - \theta_j|} \le q_{s-1}^{\frac{1}{m}}. \tag{2.6}$$

On the other hand, if $|b| > q_k|a| + (1 + q_k)M$ we observe that

$$\frac{|b - \theta_j|}{|a - \theta_j|} \ge \frac{|b| - |\theta_j|}{|a| + |\theta_j|} \ge \frac{|b| - M}{|a| + M} > q_k \ge q_k^{\frac{1}{m}} \ge q_{s-1}^{\frac{1}{m}},$$

since $q_k \ge 1$ and $q_k \ge q_{s-1}$. This contradicts (2.6), so f is the product of at most k irreducible factors over $\mathbb{Q}$.

In our second case, if we assume that $|b| > \sqrt{q_k}|a| + (1 + \sqrt{q_k})M$ and f has no rational roots, then $m \ge 2$, and consequently

$$\frac{|b - \theta_j|}{|a - \theta_j|} \ge \frac{|b| - M}{|a| + M} > \sqrt{q_k} \ge q_k^{\frac{1}{m}} \ge q_{s-1}^{\frac{1}{m}},$$

again a contradiction.

In our third case, let us assume that $q_k = 1$, $a^2 < b^2$ and $M < \frac{|a+b|}{2}$. If $b > a$, then $a + b > 0$ and the conclusion follows by Theorem 1 iii) since the disk $\{z : |z| \le M\}$ containing all the roots of f lies in the left half-plane $x < \frac{a+b}{2}$. On the other hand, if $a > b$, then $a + b < 0$ and the disk $\{z : |z| \le M\}$ lies in the right half-plane $x > \frac{a+b}{2}$, as $-M > \frac{a+b}{2}$. $\square$

3   Applications

Our first application of Theorem 3 is the following result.

Corollary 1. *Let $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$, and a, b two integers such that $a^2 < b^2$ and $|a_n| > \sum_{i=0}^{n-1} |a_i| \left(\frac{|a+b|}{2} \right)^{i-n}$. Assume that $|f(a)| = p^{k_1} r$, $|f(b)| = p^{k_2}$ with p a prime number and k_1, k_2, r integers with $k_2 > k_1 \geq 0$ and $0 < r < p$. Then f is the product of at most $1 + \lfloor (k_2 - k_1 - 1) \log_{\frac{p}{r}} p \rfloor$ irreducible factors over $\mathbb{Q}$.*

Proof.   An immediate consequence of Rouché's Theorem is that the condition $|a_n| > \sum_{i=0}^{n-1} |a_i| \left(\frac{|a+b|}{2} \right)^{i-n}$ forces all the roots of f to have absolute values less than $\frac{|a+b|}{2}$. Therefore $M < \frac{|a+b|}{2}$. Note that for every positive integer k we have $q_k \leq \tilde{q}_k$, with

$$\tilde{q}_k = \max \left\{ \frac{d_2}{d_1} \leq \sqrt[k+1]{\frac{|f(b)|}{|f(a)|}} : d_1 \mid f(a), \ d_2 \mid f(b) \right\}. \tag{3.1}$$

We search for a positive integer k as small as possible such that $\tilde{q}_k = 1$, which will also imply that $q_k = 1$. In view of (3.1) we have

$$\tilde{q}_k = \max \left\{ \frac{d_2}{d_1} \leq \sqrt[k+1]{\frac{p^{k_2-k_1}}{r}} : d_1 \mid p^{k_1} r, \ d_2 \mid p^{k_2} \right\}.$$

Observe that the least quotient $\frac{d_2}{d_1}$ that exceeds 1 with $d_1 \mid p^{k_1} r$ and $d_2 \mid p^{k_2}$ is $\frac{p}{r}$, so to prove that $\tilde{q}_k = 1$ it suffices to prove that $\frac{p}{r} > \sqrt[k+1]{\frac{p^{k_2-k_1}}{r}}$, or equivalently that $k > (k_2 - k_1 - 1) \log_{\frac{p}{r}} p$. Note that for $k_2 - k_1 > 1$ and $r > 1$, the term $(k_2 - k_1 - 1) \log_{\frac{p}{r}} p$ cannot be an integer, as p is a prime number. A suitable candidate for k is obviously $1 + \lfloor (k_2 - k_1 - 1) \log_{\frac{p}{r}} p \rfloor$, and the conclusion follows from Theorem 3.   □

We mention here that for an upper bound which depends only on p and k_2, one may use $1 + \lfloor (k_2 - 1) \log_{\frac{p}{p-1}} p \rfloor$, for instance. A special instance of Corollary 1 is the following result.

Corollary 2. *Let $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ be a polynomial with integer coefficients, with $|a_n| > 2|a_{n-1}| + 2^2|a_{n-2}| + \cdots + 2^n|a_0|$ and $a_0 \neq 0$. If $f(\mathbb{Z} \setminus \{0\})$ or $-f(\mathbb{Z} \setminus \{0\})$ contains a prime power p^k with $p > |a_0|$ and $k \geq 1$, then f is the product of at most*

$$1 + \lfloor (k-1) \log_{\frac{p}{|a_0|}} p \rfloor$$

irreducible factors over $\mathbb{Q}$.

Proof.   We will apply Corollary 1 with $a = 0$ and b an integer such that $f(b) = p^k$, so here $k_2 = k$. Since $p > |a_0| = |f(0)|$ we have $k_1 = 0$ and $r = |a_0| < p$. As $b \neq 0$ we have $|b| \geq 1$, so our assumption on the magnitude of a_n implies that

$$\begin{aligned}
|a_n| &> 2|a_{n-1}| + 2^2|a_{n-2}| + \cdots + 2^n|a_0| \\
&\geq 2|a_{n-1}| + \frac{2^2}{|b|^2}|a_{n-2}| + \cdots + \frac{2^n}{|b|^n}|a_0| = \sum_{i=0}^{n-1} |a_i| \left(\frac{|a+b|}{2} \right)^{i-n}.
\end{aligned}$$

Thus condition $|a_n| > \sum_{i=0}^{n-1} |a_i| \left(\frac{|a+b|}{2}\right)^{i-n}$ in Corollary 1 is satisfied, so we may conclude that f is the product of at most $1 + \lfloor (k-1) \log_{\frac{p}{|a_0|}} p \rfloor$ irreducible factors over $\mathbb{Q}$.   □

Another application of Theorem 3 is the following result.

Corollary 3. *Let $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$, and a, b two integers such that $a^2 < b^2$ and $|a_n| > \sum_{i=0}^{n-1} |a_i| \left(\frac{|a+b|}{2}\right)^{i-n}$. Assume that $|f(a)| = p^{k_1}$, $|f(b)| = p^{k_2} r$ with p, r prime numbers with $p > r$ and k_1, k_2 integers with $k_2 \geq k_1 > 0$. Then f is the product of at most $1 + \lfloor (k_2 - k_1) \log_r p \rfloor$ irreducible factors over $\mathbb{Q}$.*

We will prove here a more general version of Corollary 3, in which we allow r to be composite:

Corollary 4. *Let $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$, and a, b two integers such that $a^2 < b^2$ and $|a_n| > \sum_{i=0}^{n-1} |a_i| \left(\frac{|a+b|}{2}\right)^{i-n}$. Assume that $|f(a)| = p^{k_1}$, $|f(b)| = p^{k_2} r$ with p a prime number, r an integer with $0 < r < p$ and k_1, k_2 integers with $k_2 \geq k_1 > 0$. Let also q be the smallest prime factor of r. Then f is the product of at most $1 + \lfloor (k_2 - k_1) \log_q p + \log_q \frac{r}{q} \rfloor$ irreducible factors over $\mathbb{Q}$.*

Proof. Here too, all the roots of f have absolute values less than $\frac{|a+b|}{2}$, so $M < \frac{|a+b|}{2}$. In view of (3.1), we deduce in this case that

$$\tilde{q}_k = \max \left\{ \frac{d_2}{d_1} \leq \sqrt[k+1]{p^{k_2 - k_1} r} : d_1 \mid p^{k_1}, \ d_2 \mid p^{k_2} r \right\}.$$

Observe that here the least quotient $\frac{d_2}{d_1}$ that exceeds 1 with $d_1 \mid p^{k_1}$ and $d_2 \mid p^{k_2} r$ is q, so to prove that $\tilde{q}_k = 1$ it suffices to prove that $q > \sqrt[k+1]{p^{k_2 - k_1} r}$, or equivalently that

$$k > (k_2 - k_1) \log_q p + \log_q \frac{r}{q}.$$

We may therefore choose $k = 1 + \lfloor (k_2 - k_1) \log_q p + \log_q \frac{r}{q} \rfloor$, and the conclusion follows again from Theorem 3.   □

Using the well-known Eneström–Kakeya Theorem [20], saying that all the roots of a polynomial $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ with real coefficients satisfying $0 \leq a_0 \leq a_1 \leq \cdots \leq a_n$ must have absolute values at most 1, one can also prove the following results, in which we will only consider the case of positive integers a, b.

Corollary 5. *Let $f \in \mathbb{Z}[X]$ be an Eneström–Kakeya polynomial with $f(0) \neq 0$, and let a, b be two positive integers such that $f(a) = p^{k_1} r$, $f(b) = p^{k_2}$ with p a prime number and k_1, k_2, r integers with $k_2 > k_1 \geq 0$ and $0 < r < p$. Then f is the product of at most $1 + \lfloor (k_2 - k_1 - 1) \log_{\frac{p}{r}} p \rfloor$ irreducible factors over $\mathbb{Q}$.*

Proof. Here, by the Eneström–Kakeya Theorem all the roots of f must have modulus at most 1, so $M \leq 1$. Since $f(a) < f(b)$ and f has positive coefficients, we must have $a < b$, which also shows that $a + b > 2$, hence condition $M < \frac{|a+b|}{2}$ in Theorem 3 iii) is obviously satisfied. To prove that $q_k = 1$ with $k = 1 + \lfloor (k_2 - k_1 - 1) \log_{\frac{p}{r}} p \rfloor$, one may argue as in the proof of Corollary 1, and the conclusion follows by Theorem 3 iii).   □

Another result for Eneström–Kakeya polynomials is the following.

Corollary 6. *Let $f \in \mathbb{Z}[X]$ be an Eneström–Kakeya polynomial with $f(0) \neq 0$, and let a, b be two positive integers such that $f(a) = p^{k_1}$, $f(b) = p^{k_2}r$ with p, r prime numbers with $p > r$, and k_1, k_2 integers with $k_2 \geq k_1 > 0$. Then f is the product of at most $1 + \lfloor (k_2 - k_1) \log_r p \rfloor$ irreducible factors over $\mathbb{Q}$.*

Proof. We argue as before, this time using the fact that $q_k = 1$ with $k = 1 + \lfloor (k_2 - k_1) \log_r p \rfloor$, as in Corollary 3. □

One may also prove the following analogous results for Littlewood polynomials, that is for polynomials all of whose coefficients are ± 1.

Corollary 7. *Let f be a Littlewood polynomial, and a, b two nonnegative integers with $a + b \geq 4$ such that $f(a) = p^{k_1}r$, $f(b) = p^{k_2}$ with p a prime number and k_1, k_2, r integers with $k_2 > k_1 \geq 0$ and $0 < r < p$. Then f is the product of at most $1 + \lfloor (k_2 - k_1 - 1) \log_{\frac{p}{r}} p \rfloor$ irreducible factors over $\mathbb{Q}$.*

Proof. Here we use the fact that all the roots of a Littlewood polynomial have absolute values less than 2, so $M < 2$. Indeed, assume to the contrary that f would have a root θ with $|\theta| \geq 2$. Then we would obtain

$$
\begin{aligned}
0 &= |\sum_{i=0}^{n} a_i \theta^{i-n}| \geq |a_n| - \left(\sum_{i=0}^{n-1} |a_i| \cdot |\theta|^{i-n} \right) \\
&= 1 - \frac{1}{|\theta|} - \frac{1}{|\theta|^2} - \cdots - \frac{1}{|\theta|^n} \geq 1 - \frac{1}{2} - \frac{1}{2^2} - \cdots - \frac{1}{2^n} > 0,
\end{aligned}
$$

a contradiction. Since $a + b \geq 4$ and $M < 2$, condition $M < \frac{|a+b|}{2}$ in Theorem 3 iii) is obviously satisfied. Again, one proves as in Corollary 1 that we have $q_k = 1$ with $k = 1 + \lfloor (k_2 - k_1 - 1) \log_{\frac{p}{r}} p \rfloor$, and the conclusion follows by Theorem 3 iii). □

Corollary 8. *Let f be a Littlewood polynomial, and a, b two positive integers with $a + b \geq 4$ such that $f(a) = p^{k_1}$, $f(b) = p^{k_2}r$ with p, r prime numbers with $p > r$, and k_1, k_2 integers with $k_2 \geq k_1 > 0$. Then f is the product of at most $1 + \lfloor (k_2 - k_1) \log_r p \rfloor$ irreducible factors over $\mathbb{Q}$.*

Proof. Here we use the fact that $q_k = 1$ with $k = 1 + \lfloor (k_2 - k_1) \log_r p \rfloor$, and also the fact that $M < 2$. The conclusion follows again by Theorem 3 iii). □

4 The case of unitary divisors

The aim of this section is to find upper bounds for the sum of the multiplicities of the irreducible factors by studying the unitary divisors of $f(a)$ and $f(b)$. Instead of q_k given by (1.3), we will use here a potentially smaller rational number q_k^u, defined by

$$
q_k^u = \max \left\{ \frac{d_2}{d_1} \leq \sqrt[k+1]{\frac{|f(b)|}{|f(a)|}} : d_1 \in \mathcal{D}_u(f(a)), \ d_2 \in \mathcal{D}_u(f(b)) \right\}. \tag{4.1}
$$

With this notation we have the following results, that are similar to the theorems in the case of admissible divisors.

Theorem 4. *Let* $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$, *and assume that for two integers* a, b *we have* $0 < |f(a)| < |f(b)|$ *and* $\gcd(f(a), f'(a)) = \gcd(f(b), f'(b)) = 1$. *Let* k *be a positive intiger and let* q_k^u *be given by* (4.1). *Then* f *is the product of at most* k *irreducible factors over* $\mathbb{Q}$ *in each one of the following three cases:*

i) $q_k^u > 1$ *and all the roots of* f *lie inside the Apollonius circle* $\mathrm{Ap}(a, b, q_k^u)$;

ii) $q_k^u > 1$, *all the roots of* f *lie inside the Apollonius circle* $\mathrm{Ap}(a, b, \sqrt{q_k^u})$, *and* f *has no rational roots;*

iii) $q_k^u = 1$ *and either* $b > a$ *and all the roots of* f *lie in the half-plane* $x < \frac{a+b}{2}$, *or* $a > b$ *and all the roots of* f *lie in the half-plane* $x > \frac{a+b}{2}$.

Proof. Using the same notations as in the proof of Theorem 1, we observe that our assumption that $\gcd(f(a), f'(a)) = \gcd(f(b), f'(b)) = 1$ together with the divisibility conditions

$$\gcd\left(d_i, \frac{f(a)}{d_i}\right) \mid \gcd(f(a), f'(a)) \quad \text{and} \quad \gcd\left(d_i', \frac{f(b)}{d_i'}\right) \mid \gcd(f(b), f'(b))$$

imply that d_i and d_i' must be unitary divisors of $f(a)$ and $f(b)$, respectively, and this holds for each $i = 1, \ldots, s$. The proof continues as in the case of Theorem 1, except that instead of q_{s-1} and q_k we have to use here q_{s-1}^u and q_k^u, respectively, which are still greater than or equal to 1, as 1 belongs to both $\mathcal{D}_u(f(a))$ and $\mathcal{D}_u(f(b))$. $\square$

One may rephrase Theorem 4 too in a more explicit form, as follows:

Theorem 5. *Let* $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$, *and assume that for two integers* a, b *we have* $0 < |f(a)| < |f(b)|$ *and* $\gcd(f(a), f'(a)) = \gcd(f(b), f'(b)) = 1$. *Let* k *be a positive integer and let* q_k^u *be given by* (4.1). *Then* f *is the product of at most* k *irreducible factors over* $\mathbb{Q}$ *in each one of the following three cases:*

i) $q_k^u > 1$ *and each root* θ *of* f *satisfies* $\left|\theta - \frac{a(q_k^u)^2 - b}{(q_k^u)^2 - 1}\right| < q_k^u \frac{|b-a|}{(q_k^u)^2 - 1}$;

ii) $q_k^u > 1$, *each root* θ *of* f *satisfies* $\left|\theta - \frac{aq_k^u - b}{q_k^u - 1}\right| < \sqrt{q_k^u} \frac{|b-a|}{q_k^u - 1}$, *and* f *has no rational roots;*

iii) $q_k^u = 1$ *and either* $b > a$ *and all the roots of* f *lie in the half-plane* $x < \frac{a+b}{2}$, *or* $a > b$ *and all the roots of* f *lie in the half-plane* $x > \frac{a+b}{2}$.

Proof. The proof is similar to that of Theorem 2, with q_k^u instead of q_k. $\square$

We mention here that considerations as in Remark 1 apply in this case too, with q_k^u instead of q_k.

Theorem 6. *Let* $f(X) = a_0 + a_1 X + \cdots + a_n X^n$ *be a polynomial with integer coefficients,* M *the maximum of the absolute values of its roots, and assume that for two integers* a, b *we have* $0 < |f(a)| < |f(b)|$ *and* $\gcd(f(a), f'(a)) = \gcd(f(b), f'(b)) = 1$. *Let also* q_k^u *be given by relation* (4.1). *Then* f *is the product of at most* k *irreducible factors over* $\mathbb{Q}$ *in each one of the following three cases:*

i) $|b| > q_k^u |a| + (1 + q_k^u) M$;

ii) $|b| > \sqrt{q_k^u} |a| + (1 + \sqrt{q_k^u}) M$ *and f has no rational roots;*

iii) $q_k^u = 1$, $a^2 < b^2$ *and* $M < \frac{|a+b|}{2}$.

Proof. One argues as in the proof of Theorem 3, with q_k^u instead of q_k. □

In particular, we obtain the following result.

Corollary 9. *Let $f(X) = a_0 + a_1 X + \cdots + a_n X^n \in \mathbb{Z}[X]$ and a, b two integers such that $a^2 < b^2$ and $|a_n| > \sum_{i=0}^{n-1} |a_i| (\frac{|a+b|}{2})^{i-n}$. Assume that $|f(a)| = p^{k_1}$, $|f(b)| = p^{k_2} r^j$ with p, r distinct prime numbers and k_1, k_2 positive integers such $r^j > p^{k_1 - k_2}$. Assume also that $p \nmid f'(a) f'(b)$ and $r \nmid f'(b)$. Then f is the product of at most k irreducible factors over $\mathbb{Q}$ in each one of the following cases:*

i) $k_1 < k_2$, $r^j < p^{k_1}$, $r^j < p^{k_2 - k_1}$, *and* $k = 1 + \lfloor \frac{k_2 - k_1}{j} \log_r p \rfloor$;

ii) $k_1 < k_2$, $r^j > p^{k_1}$, $r^j < p^{k_2 - k_1}$, *and* $k = 1 + \lfloor \frac{k_2 \log_r p}{j - k_1 \log_r p} \rfloor$;

iii) $k_1 = k_2$, $r^j > p^{2k_1}$, *and* $k = \lfloor \frac{j}{k_1} \log_p r \rfloor$;

iv) $k_1 = k_2$, $p^{2k_1} > r^j > p^{k_1}$, *and* $k = 1 + \lfloor \frac{k_1 \log_r p}{j - k_1 \log_r p} \rfloor$;

v) $k_1 = k_2$, $r^j < p^{k_1}$, *and* $k = 1$ *(f is irreducible);*

vi) $k_1 > k_2$, $r^j < p^{k_1}$, *and* $k = 1$ *(f is irreducible);*

vii) $k_1 > k_2$, $r^j > p^{k_1 + k_2}$, *and* $k = 1 + \lfloor \frac{j \log_p r - k_1}{k_2} \rfloor$;

viii) $k_1 > k_2$, $p^{k_1} < r^j < p^{k_1 + k_2}$, *and* $k = 1 + \lfloor \frac{k_2 \log_r p}{j - k_1 \log_r p} \rfloor$.

Proof. As in the proof of Corollary 1 we have $M < \frac{|a+b|}{2}$. Note that $\mathcal{D}_u(f(a)) = \{1, p^{k_1}\}$ and $\mathcal{D}_u(f(b)) = \{1, p^{k_2}, r^j, p^{k_2} r^j\}$, so any quotient $\frac{d_2}{d_1}$ with $d_1 \in \mathcal{D}_u(f(a))$ and $d_2 \in \mathcal{D}_u(f(b))$ belongs to the set

$$S = \left\{ 1, \frac{1}{p^{k_1}}, p^{k_2}, p^{k_2 - k_1}, r^j, \frac{r^j}{p^{k_1}}, p^{k_2} r^j, p^{k_2 - k_1} r^j \right\}.$$

In each case i in the statement denote by s_i the least element of S that exceeds 1. One may check that $s_1 = r^j$, $s_2 = \frac{r^j}{p^{k_1}}$, $s_3 = p^{k_1}$, $s_4 = \frac{r^j}{p^{k_1}}$, $s_5 = r^j$, $s_6 = p^{k_2 - k_1} r^j$, $s_7 = p^{k_2}$ and $s_8 = \frac{r^j}{p^{k_1}}$. The values of k in the statement are then obtained by imposing the conditions $s_i > \sqrt[k+1]{\frac{|f(b)|}{|f(a)|}}$, that is $s_i^{k+1} > p^{k_2 - k_1} r^j$, thus forcing q_k^u to be equal to 1 in each one of the eight cases. The conclusion follows from Theorem 6. □

5   The case of multivariate polynomials

In this section we will prove some similar results for bivariate polynomials $f(X, Y)$ over an arbitrary field K. Generalizations for polynomials $f(X_1, \ldots, X_r)$ in $r \geq 3$ variables may be then obtained from the results in the bivariate case, by writing Y for X_r, X for X_{r-1}, and by replacing K with $K(X_1, \ldots, X_{r-2})$. We will recall the definition used in [5] for the admissible divisors in the bivariate case.

Definition 2. *Let K be a field, $f(X,Y) \in K[X,Y]$ and $a(X) \in K[X]$ such that $f(X,a(X)) \neq 0$. We say that a polynomial $D(X) \in K[X]$ is an admissible divisor of $f(X,a(X))$ if $D(X) \mid f(X,a(X))$ and*

$$\gcd\left(D(X), \frac{f(X,a(X))}{D(X)}\right) \mid \gcd\left(f(X,a(X)), \frac{\partial f}{\partial Y}(X,a(X))\right). \tag{5.1}$$

The set of admissible divisors of $f(X,a(X))$ will be denoted by $D_{ad}(f(X,a(X))$, and for $f(X,Y)$ and $a(X)$ as above we will denote

$$D_u(f(X,a(X))) = \left\{d \in K[X] : d(X)|f(X,a(X)),\ \gcd\left(d(X), \frac{f(X,a(X))}{d(X)}\right) = 1\right\},$$

and call it the set of unitary divisors of $f(X,a(X))$. Notice that in the particular case that $\gcd(f(X,a(X)), \frac{\partial f}{\partial Y}(X,a(X))) = 1$, $D_{ad}(f(X,a(X))$ reduces to $\mathcal{D}_u(f(X,a(X)))$.

With this definition, we have the following result, from which one may recover Theorem 5 in [5] by taking $k = 1$.

Theorem 7. *Let K be a field, $f(X,Y) = a_0(X)+a_1(X)Y+\cdots+a_n(X)Y^n \in K[X,Y]$, with $a_0,\ldots,a_n \in K[X]$, $a_0 a_n \neq 0$, and k a positive integer. Assume that for two polynomials $a(X),b(X) \in K[X]$ we have $f(X,a(X))f(X,b(X)) \neq 0$ and $\Delta_k := \frac{1}{k+1} \cdot (\deg f(X,b(X)) - \deg f(X,a(X))) \geq 0$, and let*

$$q_k = \max\{\deg d_2 - \deg d_1 \leq \Delta_k : d_1 \in D_{ad}(f(X,a(X))), d_2 \in D_{ad}(f(X,b(X)))\}.$$

If $\deg b(X) > \max\{\deg a(X), \max_{0\leq i\leq n-1} \frac{\deg a_i - \deg a_n}{n-i}\} + q_k$, then $f(X,Y)$ is the product of at most k irreducible factors over $K(X)$.

Proof. Note that once we fix the polynomials $a(X)$ and $b(X)$ as in the statement of the theorem, q_k is a decreasing function on k. Moreover, since $\Delta_k \geq 0$ and 1 is obviously an admissible divisor of both $f(X,a(X))$ and $f(X,b(X))$, a possible candidate for q_k is $0 = \deg 1 - \deg 1$, so $q_k \geq 0$ for each k. Assume towards a contradiction that one may write f as a product of $s \geq k+1$ factors $f_1,\ldots,f_s \in K[X,Y]$ that are irreducible over $K(X)$. In particular, we have

$$q_k \geq q_{s-1}. \tag{5.2}$$

Let us fix an index $i \in \{1,\ldots,s\}$ and denote

$$g_i(X,Y) := \prod_{j \neq i} f_j(X,Y).$$

We may therefore write $f = f_i \cdot g_i$ for each $i = 1,\ldots,s$. Next, since

$$\begin{aligned}
f(X,a(X)) &= f_i(X,a(X))g_i(X,a(X)) \neq 0\\
f(X,b(X)) &= f_i(X,b(X))g_i(X,b(X)) \neq 0
\end{aligned}$$

and

$$\begin{aligned}
\frac{\partial f}{\partial Y}(X,a(X)) &= \frac{\partial f_i}{\partial Y}(X,a(X))g_i(X,a(X)) + f_i(X,a(X))\frac{\partial g_i}{\partial Y}(X,a(X)),\\
\frac{\partial f}{\partial Y}(X,b(X)) &= \frac{\partial f_i}{\partial Y}(X,b(X))g_i(X,b(X)) + f_i(X,b(X))\frac{\partial g_i}{\partial Y}(X,b(X)),
\end{aligned}$$

we see that $f_i(X, a(X))$ is a divisor $d_i(X)$ of $f(X, a(X))$, and $f_i(X, b(X))$ is a divisor $d'_i(X)$ of $f(X, b(X))$ that must also satisfy the divisibility conditions

$$\gcd\left(d_i(X), \frac{f(X, a(X))}{d_i(X)}\right) \quad | \quad \gcd\left(f(X, a(X)), \frac{\partial f}{\partial Y}(X, a(X))\right) \text{ and}$$

$$\gcd\left(d'_i(X), \frac{f(X, b(X))}{d'_i(X)}\right) \quad | \quad \gcd\left(f(X, b(X)), \frac{\partial f}{\partial Y}(X, b(X))\right).$$

Therefore $d_i(X)$ and $d'_i(X)$ are admissible divisors of $f(X, a(X))$ and $f(X, b(X))$, respectively, and this holds for each $i = 1, \ldots, s$. Observe now that

$$\frac{d'_1(X)}{d_1(X)} \cdots \frac{d'_s(X)}{d_s(X)} = \frac{f(X, b(X))}{f(X, a(X))}. \tag{5.3}$$

At this point we will introduce as in [5] a nonarchimedean absolute value $|\cdot|$ on $K(X)$, as follows. We choose an arbitrary real number $\rho > 1$, and for any polynomial $A(X) \in K[X]$ we define $|A(X)|$ by

$$|A(X)| = \rho^{\deg A(X)}.$$

Then we extend the absolute value $|\cdot|$ to $K(X)$ by multiplicativity, that is, for any polynomials $A(X), B(X) \in K[X]$ with $B(X) \neq 0$, we let $\left|\frac{A(X)}{B(X)}\right| = \frac{|A(X)|}{|B(X)|}$. We note here that for any non-zero element $A(X)$ of $K[X]$ one has $|A| \geq 1$. Finally, let $\overline{K(X)}$ be a fixed algebraic closure of $K(X)$, and let us fix an extension of our absolute value $|\cdot|$ to $\overline{K(X)}$, which we will also denote by $|\cdot|$.

Applying now our absolute value to relation (5.3), we deduce that one of the quotients $\frac{|d'_1(X)|}{|d_1(X)|}, \ldots, \frac{|d'_s(X)|}{|d_s(X)|}$, say $\frac{|d'_1(X)|}{|d_1(X)|}$, must be less than or equal to $\sqrt[s]{\frac{|f(X, b(X))|}{|f(X, a(X))|}}$. In particular, we must have $\deg f_1(X, b(X)) - \deg f_1(X, a(X)) \leq \frac{1}{s}(\deg f(X, b(X)) - \deg f(X, a(X)))$, so $\deg f_1(X, b(X)) - \deg f_1(X, a(X)) \leq q_{s-1}$, or equivalently,

$$\frac{|f_1(X, b(X))|}{|f_1(X, a(X))|} \leq \rho^{q_{s-1}}. \tag{5.4}$$

Let us assume that f as a polynomial in Y with coefficients in $K[X]$ factorizes as

$$f(X, Y) = a_n(X)(Y - \xi_1) \cdots (Y - \xi_n)$$

for some $\xi_1, \ldots, \xi_n \in \overline{K(X)}$. Next, we will prove that

$$\max\{|\xi_1|, \ldots, |\xi_n|\} \leq \rho^{\max\limits_{0 \leq i \leq n-1} \frac{\deg a_i - \deg a_n}{n-i}}. \tag{5.5}$$

To this end, let $\delta := \max\limits_{0 \leq i \leq n-1} \frac{\deg a_i - \deg a_n}{n-i}$, and let us assume to the contrary that f has a root ξ with $|\xi| > \rho^\delta$. Since $\xi \neq 0$ and our absolute value also satisfies the triangle inequality, we successively deduce that

$$0 = \left|\sum_{i=0}^{n} a_i \xi^{i-n}\right| \geq |a_n| - \left|\sum_{i=0}^{n-1} a_i \xi^{i-n}\right| \geq |a_n| - \max\limits_{0 \leq i \leq n-1} |a_i| \cdot |\xi|^{i-n}$$

$$> |a_n| - \max\limits_{0 \leq i \leq n-1} |a_i| \cdot \rho^{(i-n)\delta},$$

so $|a_n| < \max\limits_{0 \leq i \leq n-1} |a_i| \cdot \rho^{(i-n)\delta}$, or equivalently

$$\deg a_n < \max_{0 \leq i \leq n-1} \{\deg a_i + (i-n)\delta\}. \tag{5.6}$$

Let us choose now an index $k \in \{0, \ldots, n-1\}$ for which the maximum in (5.6) is attained. In particular, we have $\deg a_n < \deg a_k + (k-n)\delta$, which leads us to

$$\frac{\deg a_k - \deg a_n}{n-k} > \delta = \max_{0 \leq i \leq n-1} \frac{\deg a_i - \deg a_n}{n-i},$$

a contradiction. Therefore inequality (5.5) must hold, so $|\xi_i| \leq \rho^\delta$ for $i = 1, \ldots, n$.

Assume now without loss of generality that $f_1(X,Y) = b_m(Y - \xi_1) \cdots (Y - \xi_m)$ for some $m \geq 1$ and some divisor b_m of a_n. Notice that we may write

$$\frac{f_1(X, b(X))}{f_1(X, a(X))} = \frac{b(X) - \xi_1}{a(X) - \xi_1} \cdots \frac{b(X) - \xi_m}{a(X) - \xi_m},$$

so by (5.4) we see that for at least one index $j \in \{1, \ldots, m\}$ we must have

$$\frac{|b(X) - \xi_j|}{|a(X) - \xi_j|} \leq \rho^{\frac{q_{s-1}}{m}}. \tag{5.7}$$

On the other hand, our absolute value also satisfies the triangle inequality, so

$$\frac{|b(X) - \xi_j|}{|a(X) - \xi_j|} \geq \frac{|b(X)| - |\xi_j|}{|a(X)| + |\xi_j|} \geq \frac{|b(X)| - \rho^\delta}{|a(X)| + \rho^\delta} = \frac{\rho^{\deg b(X)} - \rho^\delta}{\rho^{\deg a(X)} + \rho^\delta}.$$

All that remains now is to prove that for a sufficiently large ρ we have

$$\frac{\rho^{\deg b(X)} - \rho^\delta}{\rho^{\deg a(X)} + \rho^\delta} > \rho^{q_{s-1}} \geq \rho^{\frac{q_{s-1}}{m}},$$

which will contradict (5.7). Here the right-most inequality $\rho^{q_{s-1}} \geq \rho^{\frac{q_{s-1}}{m}}$ obviously holds for an arbitrary $\rho > 1$ since $q_{s-1} \geq 0$ and $m = \deg_Y f_1 \geq 1$. The first inequality is equivalent to

$$\rho^{\deg b(X)} > \rho^{q_{s-1} + \deg a(X)} + \rho^{q_{s-1} + \delta} + \rho^\delta,$$

which will obviously hold for a sufficiently large ρ, since by our assumption on the magnitude of $\deg b(X)$ we have $\deg b(X) > \max\{q_k + \deg a(X), q_k + \delta, \delta\}$, and $q_k \geq q_{s-1}$, according to (5.2). Therefore one may write f as a product of at most k irreducible factors over $K(X)$, and this completes the proof of the theorem. □

In particular, for $a(X) = 0$ and $b(X)$ denoted by $g(X)$, we obtain from Theorem 7 the following result:

Corollary 10. *Let K be a field, $f(X,Y) = a_0(X) + a_1(X)Y + \cdots + a_n(X)Y^n \in K[X,Y]$, with $a_0, a_1, \ldots, a_n \in K[X]$, $a_0 a_n \neq 0$, $a_0 \in K$ and*

$$\deg a_{n-1} \geq \deg a_n \geq \max\{\deg a_0, \deg a_1, \ldots, \deg a_{n-2}\}.$$

If $f(X, g(X)) = h(X)^k$ for $g, h \in K[X]$ with $\deg g > \deg a_{n-1} - \deg a_n$, h irreducible and k a positive integer, then $f(X,Y)$ is the product of at most k irreducible factors over $K(X)$.

Proof.   We apply Theorem 7 with $a(X) = 0$ and $b(X) = g(X)$. Since $f(X, a(X)) = a_0 \in K \setminus \{0\}$ we have $\deg f(X, a(X)) = 0$, and since $f(X, b(X)) = h(X)^k$ with h irreducible over K and $k \geq 1$, we have $\deg f(X, b(X)) = k \deg h \geq 1$. Therefore $\Delta_k = \frac{1}{k+1}(\deg f(X, b(X)) - \deg f(X, a(X))) = \frac{k}{k+1} \deg h > 0$. Our assumption that

$$\deg a_{n-1} \geq \deg a_n \geq \max\{\deg a_0, \deg a_1, \ldots, \deg a_{n-2}\}$$

shows that condition $\deg b(X) > \max\{\deg a(X), \max_{0 \leq i \leq n-1} \frac{\deg a_i - \deg a_n}{n-i}\} + q_k$ reduces in this case to $\deg b(X) > \deg a_{n-1} - \deg a_n + q_k$. It remains to prove that $q_k = 0$. To prove this, we notice that any divisor d_2 of $f(X, b(X)) = h(X)^k$ is a power of h, as h is irreducible, while any divisor d_1 of $f(X, a(X))$ is a constant, as $a_0 \in K$. Thus, the least positive value of $\deg d_2 - \deg d_1$ with $d_2 \mid f(X, b(X))$ and $d_1 \mid f(X, a(X))$ is $\deg h$, and since $\Delta_k = \frac{k}{k+1} \deg h < \deg h$, we conclude that $q_k = 0$, which completes the proof.   □

We end this section with a result that requires knowing only the unitary divisors of $f(X, a(X))$ and $f(X, b(X))$, provided $f(X, a(X))$ and $\frac{\partial f}{\partial Y}(X, a(X))$ are relatively prime, and $f(X, b(X))$ and $\frac{\partial f}{\partial Y}(X, b(X))$ are also relatively prime.

Theorem 8. *Let K be a field, $f(X, Y) = a_0(X) + a_1(X)Y + \cdots + a_n(X)Y^n \in K[X, Y]$, with $a_0, \ldots, a_n \in K[X]$, $a_0 a_n \neq 0$, and k a positive integer. Assume that for two polynomials $a(X), b(X) \in K[X]$ we have $f(X, a(X))f(X, b(X)) \neq 0$ and $\Delta_k := \frac{1}{k+1} \cdot (\deg f(X, b(X)) - \deg f(X, a(X))) \geq 0$, and let*

$$q_k^u = \max\{\deg d_2 - \deg d_1 \leq \Delta_k : d_1 \in D_u(f(X, a(X))), d_2 \in D_u(f(X, b(X)))\}.$$

If $\gcd(f(X, a(X)), \frac{\partial f}{\partial Y}(X, a(X))) = 1$, $\gcd(f(X, b(X)), \frac{\partial f}{\partial Y}(X, b(X))) = 1$ and

$$\deg b(X) > \max\left\{\deg a(X), \max_{0 \leq i \leq n-1} \frac{\deg a_i - \deg a_n}{n-i}\right\} + q_k^u,$$

then $f(X, Y)$ is the product of at most k irreducible factors over $K(X)$.

Proof.   Here, with the same notations as in the proof of Theorem 7, we see that $d_i(X)$ must belong to $\mathcal{D}_u(f(X, a(X)))$, while $d_i'(X)$ must belong to $\mathcal{D}_u(f(X, b(X)))$. We notice here that we will still have $q_k^u \geq 0$, since 1 belongs to both $\mathcal{D}_u(f(X, a(X)))$ and $\mathcal{D}_u(f(X, b(X)))$. The rest of the proof is similar to that of Theorem 7, and will be omitted.   □

6   Examples

1) To show that in some cases our results are sharp, we will first consider the following example. Let $p \geq 7$ be a prime number, and let $f(X) = p(p-1)X^3 + X^2 + (p-2)X + 1$. We will apply Corollary 2 by observing that $f(1) = p^2$, $a_0 = 1$, so $k = 2$ and $1 + \lfloor (k-1) \log_{\frac{p}{|a_0|}} p \rfloor = 2$. The condition $|a_n| > 2|a_{n-1}| + 2^2|a_{n-2}| + \cdots + 2^n|a_0|$ reduces in our case to the inequality $p(p-1) > 2 + 4(p-2) + 8$, that is to $p^2 > 5p + 2$, which holds for primes $p \geq 7$. We may thus conclude that f is the product of at most two irreducible factors over

$\mathbb{Q}$. On the other hand, we notice that f may be written as $(pX^2 - X + 1)((p-1)X + 1)$, so it has two irreducible factors.

2) For another simple example where our results provide sharp estimates, this time with $q_2 > 1$, consider the polynomial $f(X) = 35X^4 + 12X^2 + 1$, and let us pretend that we don't know how to factor it. One may check that f has no rational roots. Without computing the roots of f, we are going to test the conditions in Theorem 2 ii) with $a = 1$ and $b = 2$. We have $f(1) = 2^4 \cdot 3$ and $f(2) = 3 \cdot 7 \cdot 29$, and one may deduce that $q_2 = \frac{29}{16} = 1.8125$. Instead of asking all the roots θ of f to satisfy condition $|\theta - \frac{aq_2 - b}{q_2 - 1}| < \sqrt{q_2}\frac{|b-a|}{q_2-1}$, it suffices to check that they satisfy $|\theta| < \sqrt{q_2}\frac{|b-a|}{q_2-1} - \frac{|aq_2-b|}{q_2-1} \approx 1.4262$. Since $35 > 12 + 1$, we deduce by Rouché' s Theorem that all the roots of f have absolute values less than 1, and we conclude by Theorem 2 ii) that f is the product of at most two irreducible factors over $\mathbb{Q}$.

3) Let us fix any arbitrarily chosen integers $a_1, \ldots, a_{n-1}$ and $k \geq 0$. Then for all but finitely many prime numbers p the polynomial

$$f(X) = 2p^k + a_1 X + \cdots + a_{n-1}X^{n-1} + (p^{k+2} - 2p^k - a_1 - \cdots - a_{n-1})X^n$$

is the product of at most two irreducible factors over $\mathbb{Q}$.

To prove this, observe that $f(0) = 2p^k$ and $f(1) = p^{k+2}$, so we may apply Corollary 1 with $a = 0$, $b = 1$, $k_1 = k$, $k_2 = k + 2$, $r = 2$, and $1 + \lfloor (k_2 - k_1 - 1) \log_{\frac{r}{r}} p \rfloor = 2$, since $1 < \log_{\frac{r}{r}} p < 2$ for $p \geq 5$. It remains to prove that the leading coefficient of f satisfies the inequality

$$|p^{k+2} - 2p^k - a_1 - \cdots - a_{n-1}| > 2^{n+1}p^k + \sum_{i=1}^{n-1} 2^{n-i}|a_i|,$$

and this obviously holds for sufficiently large prime numbers p.

For an example where an explicit lower bound for p can be easily obtained, one can take $|a_1| = \cdots = |a_{n-1}| = 1$ and $k \geq 2$ to conclude that f is the product of at most two irreducible factors over $\mathbb{Q}$ for all primes $p \geq 2^{\frac{n+1}{2}} + 1$. Indeed, since $|a_n| \geq p^{k+2} - 2p^k - n + 1$ and $\sum_{i=0}^{n-1} 2^{n-i}|a_i| = 2^n - 2 + 2^{n+1}p^k$, it suffices to ask p to satisfy $p^2 > 2 + 2^{n+1} + \frac{2^n + n - 3}{p^k}$, which will obviously hold for $p \geq 2^{\frac{n+1}{2}} + 1$.

4) Let p be a prime number and consider the polynomial $f(X, Y) \in \mathbb{Z}[X, Y]$ given by

$$(pX + 1)^2 Y^4 + (2p - 2)(pX^2 + X)Y^3 + [(p-1)^2 X^2 + 2pX + 2]Y^2 + (2p - 2)XY + 1.$$

Notice that f is written as a polynomial in Y with coefficients in $\mathbb{Z}[X]$, namely $f = \sum_{i=0}^{4} a_i(X)Y^i$ with $a_i(X) \in \mathbb{Z}[X]$, and we have $\deg a_4 = \deg a_3 = \deg a_2 = 2$, $\deg a_1 = 1$, and $\deg a_0 = 0$, so condition

$$\deg a_{n-1} \geq \deg a_n \geq \max\{\deg a_0, \deg a_1, \ldots, \deg a_{n-2}\}$$

in Corollary 10 is satisfied. On the other hand, we observe that

$$\begin{aligned} f(X, X) &= p^2 X^6 + 2p^2 X^5 + p^2 X^4 + 2pX^3 + 2pX^2 + 1 \\ &= (pX^3 + pX^2 + 1)^2, \end{aligned}$$

which is the square of an Eisensteinian polynomial with respect to the prime p. We may thus apply Corollary 10 with $g(X) = X$, which satisfies the condition $\deg g > \deg a_{n-1} - \deg a_n$,

and with $h(X) = pX^3 + pX^2 + 1$, which is irreducible over $\mathbb{Q}$. We conclude that f is the product of at most two irreducible factors over $\mathbb{Q}(X)$. Indeed, one may check that in fact we have $f(X, Y) = ((pX + 1)Y^2 + (p - 1)XY + 1)^2$, so $(pX + 1)Y^2 + (p - 1)XY + 1$ must be irreducible over $\mathbb{Q}(X)$, which may also be tested directly, or again by Corollary 10.

References

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

[2] P. Batra, M. Mignotte, D. Ştefănescu, Improvements of Lagrange's bound for polynomial roots, *J. Symbolic Comput.*, **82**, 19–25 (2017).

[3] A. Bodin, P. Dèbes, S. Najib, Prime and coprime values of polynomials, *Enseign. Math.*, **66**, 169–182 (2020).

[4] A. I. Bonciocat, N. C. Bonciocat, The irreducibility of polynomials that have one large coefficient and take a prime value, *Canad. Math. Bull.*, **52**, 511–520 (2009).

[5] A. I. Bonciocat, N. C. Bonciocat, Y. Bugeaud, M. Cipu, Apollonius circles and irreducibility criteria for polynomials, *Indag. Math.*, **33**, 421–439 (2022).

[6] A. I. Bonciocat, N. C. Bonciocat, A. Zaharescu, On the irreducibility of polynomials that take a prime power value, *Bull. Math. Soc. Sci. Math. Roumanie*, **54 (102)**, 41–54 (2011).

[7] N. C. Bonciocat, Upper bounds for the number of factors for a class of polynomials with rational coefficients, *Acta Arith.*, **113**, 175–187 (2004).

[8] J. Brillhart, M. Filaseta, A. Odlyzko, On an irreducibility theorem of A. Cohn, *Canad. J. Math.*, **33**, 1055–1059 (1981).

[9] M. Cavachi, On a special case of Hilbert's irreducibility theorem, *J. Number Theory*, **82**, 96–99 (2000).

[10] M. Cavachi, M. Vâjâitu, A. Zaharescu, A class of irreducible polynomials, *J. Ramanujan Math. Soc.*, **17**, 161–172 (2002).

[11] M. Cole, S. Dunn, M. Filaseta, Further irreducibility criteria for polynomials with non-negative coefficients, *Acta Arith.*, **175**, 137–181 (2016).

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

[13] V. F. COWLING, W. J. THRON, Zero-free regions of polynomials, *J. Indian Math. Soc. (N.S.)*, **20**, 307–310 (1956).

[14] H. L. DORWART, Irreducibility of polynomials, *Amer. Math. Monthly*, **42**, 369–381 (1935).

[15] M. FILASETA, A further generalization of an irreducibility theorem of A. Cohn, *Canad. J. Math.*, **34**, 1390–1395 (1982).

[16] M. FILASETA, Irreducibility criteria for polynomials with non-negative coefficients, *Canad. J. Math.*, **40**, 339–351 (1988).

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

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

[19] N. H. GUERSENZVAIG, Simple arithmetical criteria for irreducibility of polynomials with integer coefficients, *Integers*, **13**, 1–21 (2013).

[20] S. KAKEYA, On the limits of the roots of an algebraic equation with positive coefficients, *Tohoku Mathematical Journal (First Series)*, **2**, 140–142 (1912).

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

[22] M. MARDEN, *Geometry of polynomials*, Mathematical Surveys and Monographs no. 3, American Mathematical Society, Providence, RI (1966).

[23] M. MIGNOTTE, An inequality on the greatest roots of a polyomial, *Elem. Math.*, **46**, 85–86 (1991).

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

[25] O. PERRON, *Algebra II. Theorie der algebraischen Gleichungen*, Walter de Gruyter & Co., Berlin (1951).

[26] G. PÓLYA, G. SZEGÖ, *Aufgaben und Lehrsätze aus der Analysis*, Springer-Verlag, Berlin (1964).

[27] M. RAM MURTY, Prime numbers and irreducible polynomials, *Amer. Math. Monthly*, **109**, 452–458 (2002).

[28] P. STÄCKEL, Arithmetischen Eigenschaften ganzer Funktionen, *Journal für Mathematik*, **148**, 101–112 (1918).

[29] L. Weisner, Criteria for the irreducibility of polynomials, *Bull. Amer. Math. Soc.*, **40**, 864–870 (1934).

[1] Simion Stoilow Institute of Mathematics of the Romanian Academy, Research Unit 3,
P.O. Box 1-764, Bucharest 014700, Romania
E-mail: `Anca.Bonciocat@imar.ro`

[2] Simion Stoilow Institute of Mathematics of the Romanian Academy, Research Unit 7,
P.O. Box 1-764, Bucharest 014700, Romania
E-mail: `Nicolae.Bonciocat@imar.ro`

[3] Université de Strasbourg, Mathématiques, 7, rue René Descartes,
67084 Strasbourg Cedex, France
E-mail: `yann.bugeaud@math.unistra.fr`

[4] Simion Stoilow Institute of Mathematics of the Romanian Academy, Research Unit 7,
P.O. Box 1-764, Bucharest 014700, Romania
E-mail: `Mihai.Cipu@imar.ro`

[5] Université de Strasbourg, Mathématiques, 7, rue René Descartes,
67084 Strasbourg Cedex, France
E-mail: `maurice.mignotte@math.unistra.fr`