Bull. Math. Soc. Sci. Math. Roumanie
Tome 65 (113), No. 2, 2022, 149–180

Irreducibility criteria for some classes of compositions of polynomials with integer coefficients

by

Ciprian Mircea Bonciocat[(1)], Nicolae Ciprian Bonciocat[(2)], Yann Bugeaud[(3)],
Mihai Cipu[(4)], Maurice Mignotte[(5)]

Dedicated to the memory of Professor Doru Ştefănescu

Abstract

We provide irreducibility criteria for compositions of polynomials with integer coefficients, of the form $f \circ g(X)$, for the case that f has leading coefficient divisible by the k^{th} power of a sufficiently large prime number, and k is coprime to $\deg f$ and $\deg g$.

Key Words: Irreducible polynomial, resultant, prime number.
2020 Mathematics Subject Classification: Primary 11R09; Secondary 11C08.

1 Introduction

Many of the classical irreducibility criteria refer to the class of compositions of polynomials. The earliest such results in the univariate case appeared in the works of Schur [17], Pólya [49], Flügel [34], Ille [43], A. Brauer, R. Brauer and Hopf [18], Wegner [58], Dorwart and Ore [31]. Further irreducibility results for compositions of polynomials appeared in papers by Seres [53], [54], [55] and Győry [37], [38], [39], [40], [41]. More recent irreducibility criteria for compositions of polynomials can be found in papers by Guersenzvaig [36], Győry, Hajdu and Tijdeman [42], Ayad [1], and also in [10], [15] and [16]. Many fundamental results on the reduction, specialization and composition of polynomials in connection with the Hilbert Irreducibility Theorem, Bertini-Noether Theorem and Schinzel Hypothesis appeared in the last decades, and here we will mention, for instance, the results of Fried [35], Sprindžuk [56], Dèbes [25], [26], [27], [28] and [29], Morita [45], Langmann [44], Cavachi [21], Müller [46], Dvornicich and Zannier [33], Corvaja [24], Dèbes and Walkowiak [30], Zannier [59], Bary-Soroker [2], Castillo and Dietmann [20], Bary-Soroker and Entin [3], and Bodin, Dèbes and Najib [4], [5] and [6]. Many of these results provide valuable techniques and ideas useful in the difficult problem of testing the irreducibility of compositions of polynomials, in both univariate and multivariate cases.

One way to study compositions of polynomials $f \circ g(X)$ over unique factorization domains, with $f(X) = a_nX^n + \cdots + a_1X + a_0$ and $a_0a_n \neq 0$, is to regard them as linear combinations of two relatively prime polynomials F and G, by writing

$$f \circ g(X) = a_nF(X) + G(X),$$

with $F = g^n$ and $G = a_0 + a_1g + \cdots + a_{n-1}g^{n-1}$. One method to test the irreducibility of a linear combination of two relatively prime polynomials was studied by Cavachi [21], which, inspired by some results of Fried [35] and Langmann [44] on Hilbert's Irreducibility Theorem, proved that a linear combination $pF(X) + G(X)$, with F, G relatively prime polynomials with rational coefficients and $\deg G < \deg F$, is irreducible over $\mathbb{Q}$ for all but finitely many prime numbers p. Cavachi, M. Vâjâitu and Zaharescu [22] obtained an explicit lower bound for the primes that ensure the irreducibility of the linear combination, depending on the degrees of F and G and on their coefficients (see [23] for the multivariate case). Sharper bounds and results for the case that $\deg F = \deg G$ have been obtained later in [12]. The idea to study compositions of polynomials by regarding them as linear combinations of polynomials was used in the univariate case in [10], and also in [7], [8] and [9], where the more general concept of multiplicative convolutions of polynomials was studied. For instance, the following result for compositions of polynomials with integer coefficients was proved in [10].

Theorem A ([10, Corollary 4]) *Let $F(X) = \sum_{i=0}^{m} a_i X^i$ and $G(X) = \sum_{i=0}^{n} b_i X^i \in \mathbb{Z}[X]$ be non-constant polynomials of degrees m and n respectively, with $a_0 \neq 0$. If $a_m = pq$ with p a prime satisfying*

$$p > \max\left\{ |q|^{m-1} L^*\left(F\left(\frac{X}{|q|}\right)\right),\ |q|^{n-1}|b_n|^{mn} L^*\left(F\left(\frac{X}{|q|^{n/m}|b_n|^n}\right)\right)\right\},$$

then the polynomial $F \circ G$ is irreducible over $\mathbb{Q}$.

Here and henceforth we use the following definition:

Definition 1. *For a complex polynomial F, $L^*(F)$ stands for the sum of the absolute values of the coefficients of F, except for the leading one.*

An irreducibility criterion that complements Theorem A, which uses similar ideas, as well as a Newton polygon argument, is the following result proved in [8].

Theorem B. ([8, Corollary 1.4]) *Let $f(X) = a_0 + a_1 X + \cdots a_m X^m$ and $g(X) = b_0 + b_1 X + \cdots + b_n X^n \in \mathbb{Z}[X]$ be polynomials of degrees $m \geq 1$ and $n \geq 1$ respectively, $a_0 \neq 0$. Put*

$$d = \max\{i :\ i < m \ \text{ and } \ a_i \neq 0\}$$

and assume that $a_m = p^k q$ with p a prime number, q a non-zero integer, $p \nmid q a_d b_n$ and k a positive integer coprime to $(m-d)n$. If

$$|a_m| > \max\left\{ \sum_{i=0}^{d} |a_i| \cdot |q|^{m-i},\ \sum_{i=0}^{d} |a_i| \cdot [|q|^{\frac{n}{m}} |b_n|^n]^{m-i} \right\},$$

then the polynomial $f \circ g$ is irreducible over $\mathbb{Q}$.

We refer the interested reader to [11] and [14] for more irreducibility criteria analogous to Theorems A and B, concerning multivariate polynomials over arbitrary fields in non-Archimedean settings instead.

The aim of this paper is to complement Theorem A and Theorem B, by proving several irreducibility criteria for the case that $a_m = p^k q$ with p prime, q an integer not divisible by p, and k a positive integer coprime to mn. Unlike Theorem B, the results in this paper will not rely on a Newton polygon argument, but instead will require a simultaneous analysis of some resultants associated to the hypothetical factors of $f \circ g(X)$. For some additional irreducibility criteria that rely on Newton polygons and resultants we refer the interested reader to Ştefănescu [57], and Panaitopol and Ştefănescu [47], [48].

To get a glimpse of the results that may be obtained by the methods employed in this paper, we will mention the following two irreducibility criteria, that are simple instances of more general results appearing in the following two sections of the paper.

Corollary 7 *Let $f(X) = a_0 + a_1X + \cdots + a_mX^m$ and $g(X) = b_0 + b_1X + \cdots + b_nX^n$ be polynomials with integer coefficients, of degrees $m \geq 2$ and $n \geq 2$, with $a_0 \neq 0$ and $|b_n| = 1$. Assume that $|a_m| = p^k$, where p is a prime number and k is coprime to mn. If*

$$p > (|a_0| + |a_1| + \cdots + |a_{m-1}|)^{\max\{m,n\}-1},$$

then the polynomial $f \circ g$ is irreducible over $\mathbb{Q}$.

Corollary 11 *Let $f(X) = a_0 + \cdots + a_mX^m$ and $g(X) = b_0 + \cdots + b_nX^n$ be polynomials with integer coefficients, of degrees $m \geq 3$ and $n \geq 3$, with $a_0 \neq 0$ and $|b_n| = 1$. Assume that $a_m = p^k$, where p is a prime number and k satisfies $k \equiv 1 \pmod{m}$ and $k \equiv 1 \pmod{n}$. If*

$$p > (|a_0| + |a_1| + \cdots + |a_{m-1}|)^{\frac{\max\{m,n\}-1}{2}},$$

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

In the proof of some of our results we will need the following famous result by Capelli, which is one of the fundamental tools to study the canonical factorization for compositions of polynomials:

Theorem. *Let K be a field, $f, g \in K[X]$, f irreducible over K, $f(\alpha) = 0$. If*

$$g(X) - \alpha \quad \underset{K(\alpha)}{\overset{can}{=}} \quad const \cdot \prod_{i=1}^{r} \phi_i(X)^{e_i}, \qquad \textit{then}$$

$$f \circ g(X) \quad \underset{K}{\overset{can}{=}} \quad const \cdot \prod_{i=1}^{r} N_{K(\alpha)/K}\phi_i(X)^{e_i}.$$

In particular, the degree of every irreducible factor of $f \circ g$ must be a multiple of $\deg f$.

Here the notation $F \underset{K}{\overset{can}{=}} const \cdot \prod_{i=1}^{r} \phi_i(X)^{e_i}$ stands for the fact that the ϕ_i's are irreducible over K and prime to each other, so that the factorization is *canonical.* We mention here that Capelli [19] proved this result for $K \subset \mathbb{C}$, Rédei [50] proved it for the case of a separable f, while in its general form, this result first appeared in the book of Schinzel [51] (see also [52]).

The paper is structured as follows. The following section provides irreducibility criteria for the case that k is coprime to mn, but no specific information is known on the inverse of k modulo mn, or on the residue class of k modulo mn. A deeper analysis leading to sharper irreducibility conditions is done in Section 3 and Section 4, for the cases that the inverse of k modulo mn and the remainder of the Euclidean division of k by mn are known, respectively. Several examples are given in the last section of the paper.

We end this section by mentioning that throughout the paper, the signs of the coefficients of f and g are irrelevant, so we may arbitrarily change them, without affecting the conclusions in our results.

2 The case that no additional information on k is known

Our first result that requires no information on the residue class of k modulo mn is:

Theorem 1. *Let $f(X)=a_0+a_1X+\cdots+a_mX^m$ and $g(X)=b_0+b_1X+\cdots+b_nX^n$ be non-constant polynomials with integer coefficients, satisfying $a_0a_mb_n\neq 0$. If $a_m=p^kq$ with p a prime number, q an integer, k a positive integer coprime to mn, and*

$$p>|b_n|^{m^2n}\cdot\min\{|q|,L^*(f(\lambda X))\}\cdot\max\{|q|,L^*(f(\lambda X))\}^{mn-1},$$

with $\lambda=(|b_n|^{mnk}|a_0|^{\frac{k-1}{m}}|q|^{\frac{k+1}{m}}\cdot\max\{|a_0|,|q|\}^{\frac{(mn-2)k}{m}})^{-1}$, then $f\circ g$ is irreducible over $\mathbb{Q}$.

We note here that in the non-trivial case that at least one of m and n is greater than 1, the positive real λ in Theorem 1 is at most 1, and can be quite small for some values of $|q|$, $|b_n|$, $|a_0|$, m or n, thus making the assumption on the magnitude of p reasonably sharp. When we are not particularly interested in finding small primes p that guarantee the irreducibility of $f\circ g$, we may use instead of Theorem 1 the following simpler, but weaker result.

Corollary 1. *Let $f(X)=a_0+a_1X+\cdots+a_mX^m$ and $g(X)=b_0+b_1X+\cdots+b_nX^n$ be non-constant polynomials with integer coefficients, satisfying $a_0a_mb_n\neq 0$. If $a_m=p^kq$ with p a prime number, q an integer, k a positive integer coprime to mn, and*

$$p>|b_n|^{m^2n}\cdot\min\{|q|,|a_0|+\cdots+|a_{m-1}|\}\cdot\max\{|q|,|a_0|+\cdots+|a_{m-1}|\}^{mn-1},$$

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

We mention that in some cases, unlike the condition on p in Corollary 1, the one in Theorem 1 allows the coefficients $a_1,\dots,a_{m-1}$ to be divisible by p as well. The reason is that when $mn>1$ and at least one of $|b_n|$, $|a_0|$ or $|q|$ is larger than 1, the value of λ in the statement of Theorem 1 can be made arbitrarily small by simply increasing k, while keeping it coprime to mn. As a consequence, for sufficiently large such k, $L^*(f(\lambda X))$ can be arbitrarily close to $|a_0|$, no matter what values we choose for the coefficients $a_1,\dots,a_{m-1}$. To illustrate this situation, we will prove the following result.

Corollary 2. *Let $f(X)=a_0+a_1X+\cdots+a_mX^m$ and $g(X)=b_0+b_1X+\cdots+b_nX^n$ be non-constant polynomials with integer coefficients, satisfying $a_0a_mb_n\neq 0$. Assume that $a_m=p^kq$ with p a prime number, q an integer, and k a positive integer. If $|a_0qb_n|>1$ and*

$$p>|b_n|^{m^2n}\cdot\min\{|q|,|a_0|\}\cdot\max\{|q|,|a_0|\}^{mn-1},$$

then $f\circ g$ is irreducible over $\mathbb{Q}$ for sufficiently large integers k coprime to mn.

In particular, for $g(X)=X$ we obtain from Theorem 1 the following irreducibility criterion for polynomials with integer coefficients:

Corollary 3. *Let $f(X)=a_0+a_1X+\cdots+a_mX^m$ be a non-constant polynomial with integer coefficients, satisfying $a_0a_m\neq 0$. If $a_m=p^kq$ with p a prime number, q an integer, k a positive integer coprime to m, and*

$$p>\min\{|q|,L^*(f(\lambda X))\}\cdot\max\{|q|,L^*(f(\lambda X))\}^{m-1},$$

with $\lambda=(|a_0|^{\frac{k-1}{m}}|q|^{\frac{k+1}{m}}\cdot\max\{|a_0|,|q|\}^{\frac{(m-2)k}{m}})^{-1}$, then f is irreducible over $\mathbb{Q}$.

Two simple, explicit instances of Corollary 3 appear in the following results.

Corollary 4. *Let $f(X) = a_0 + a_1X + \cdots + a_mX^m$ be a polynomial with integer coefficients of degree $m \geq 2$, $a_0 \neq 0$. Assume that $a_m = p^kq$ with p a prime number, q an integer satisfying $|q| > |a_0|$, and k a positive integer coprime to m. If $p > (1 + |a_0|) \cdot |q|^{m-1}$ and*

$$k > \log_{|a_0|^{\frac{1}{m}}|q|^{\frac{m-1}{m}}}(|a_1| + \cdots + |a_{m-1}|),$$

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

Corollary 5. *Let $f(X) = a_0 + a_1X + \cdots + a_mX^m$ be a polynomial with integer coefficients of degree $m \geq 2$, satisfying $a_0 \neq 0$. Assume that $a_m = p^kq$ with p a prime number, q an integer with $1 < |q| \leq |a_0|$, and k a positive integer coprime to m. If $p > (1 + |a_0|)^{m-1}|q|$ and*

$$k > 1 + \log_{|a_0|^{\frac{m-1}{m}}|q|^{\frac{1}{m}}}(|a_1| + \cdots + |a_{m-1}|),$$

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

A comparison between the irreducibility conditions in Corollary 4, Corollary 5 and those in Dumas' irreducibility criterion is in order. We recall the famous irreducibility criterion of Dumas [32], that generalizes the Schönemann-Eisenstein irreducibility criterion.

Irreducibility criterion of Dumas *Let $f(X) = a_0 + a_1X + \cdots + a_mX^m$ be a polynomial with integer coefficients, and let p be a prime number. If*

i) $\frac{\nu_p(a_i)}{i} > \frac{\nu_p(a_m)}{m}$ *for $i = 1, \ldots, m-1$,*
ii) $\nu_p(a_0) = 0$,
iii) $\gcd(\nu_p(a_m), m) = 1$,

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

Here, for an integer n and a prime number p, $\nu_p(n)$ stands for the largest integer i such that $p^i \mid n$ (by convention, $\nu_p(0) = \infty$). We observe that in Dumas' criterion the multiplicities of p in the prime factorizations of the coefficients a_i, $i = 1, \ldots, m-1$, must exceed a certain lower bound linear in i, more precisely they must satisfy the inequality $\nu_p(a_i) > \frac{i}{m} \cdot \nu_p(a_m)$, while $k := \nu_p(a_m)$ is coprime to m, and a_0 is not divisible by p. In Corollary 4 and Corollary 5 there is no restriction on $\nu_p(a_i)$ for $i = 1, \ldots, m-1$, but this additional flexibility in choosing the coefficients comes at the cost of asking p and k to exceed certain explicit lower bounds, while in Corollary 3 there is no restriction on k other than being coprime to m, and p is asked to exceed a lower bound potentially larger than in Corollary 4 and Corollary 5.

We may relax the conditions on k and p in the statement of Theorem 1 if we already know that f is irreducible, as shown in the following result:

Theorem 2. *Let $f(X) = a_0 + a_1X + \cdots + a_mX^m$ and $g(X) = b_0 + b_1X + \cdots + b_nX^n$ be non-constant polynomials with integer coefficients, with $a_0a_mb_n \neq 0$ and f irreducible over $\mathbb{Q}$. If $a_m = p^kq$ with p a prime number, q an integer, k a positive integer coprime to n, and*

$$p > |b_n|^{mn} \cdot \min\{|q|, L^*(f(\lambda X))\} \cdot \max\{|q|, L^*(f(\lambda X))\}^{n-1},$$

with $\lambda = (|b_n|^{nk}|a_0|^{\frac{k-1}{m}}|q|^{\frac{k+1}{m}} \cdot \max\{|a_0|, |q|\}^{\frac{(n-2)k}{m}})^{-1}$, then $f \circ g$ is irreducible over $\mathbb{Q}$.

By combining Corollary 3 and Theorem 2 we obtain the following irreducibility criterion that no longer requires the assumption that f is irreducible:

Theorem 3. *Let $f(X)=a_0+a_1X+\cdots+a_mX^m$ and $g(X)=b_0+b_1X+\cdots+b_nX^n$ be non-constant polynomials with integer coefficients, with $a_0a_mb_n\neq 0$. Assume that $a_m=p^kq$ with p a prime number, q an integer, and k a positive integer coprime to mn. If*

$$p>\max\left\{\min\{|q|,L^*(f(\lambda_1X))\}\cdot\max\{|q|,L^*(f(\lambda_1X))\}^{m-1},\right.$$
$$\left.|b_n|^{mn}\cdot\min\{|q|,L^*(f(\lambda_2X))\}\cdot\max\{|q|,L^*(f(\lambda_2X))\}^{n-1}\right\},$$

with

$$\begin{aligned}\lambda_1&=\left(|a_0|^{\frac{k-1}{m}}|q|^{\frac{k+1}{m}}\cdot\max\{|a_0|,|q|\}^{\frac{(m-2)k}{m}}\right)^{-1}\quad\text{and}\\ \lambda_2&=\left(|b_n|^{nk}|a_0|^{\frac{k-1}{m}}|q|^{\frac{k+1}{m}}\cdot\max\{|a_0|,|q|\}^{\frac{(n-2)k}{m}}\right)^{-1},\end{aligned}$$

then the polynomial $f\circ g$ is irreducible over $\mathbb{Q}$.

Even if the lower bound on p in Theorem 3 is quite involved, it takes simpler and more explicit forms when some additional information on the coefficients and on the degrees of f and g is known. We will only state here two results corresponding to the case that $|b_n|=1$ and $m=n$, and to the case that $|b_n|=|q|=1$, respectively:

Corollary 6. *Let $f(X)=a_0+a_1X+\cdots+a_mX^m$ and $g(X)=b_0+b_1X+\cdots+b_mX^m$ be non-constant polynomials with integer coefficients, with $|b_m|=1$, and $a_m=p^kq$ with p a prime number, q a nonzero integer, and k a positive integer coprime to m. If*

$$p>\min\{|q|,L^*(f(\lambda X))\}\cdot\max\{|q|,L^*(f(\lambda X))\}^{m-1},$$

with $\lambda=(|a_0|^{\frac{k-1}{m}}|q|^{\frac{k+1}{m}}\cdot\max\{|a_0|,|q|\}^{\frac{(m-2)k}{m}})^{-1}$, then $f\circ g$ is irreducible over $\mathbb{Q}$.

Corollary 7. *Let $f(X)=a_0+a_1X+\cdots+a_mX^m$ and $g(X)=b_0+b_1X+\cdots+b_nX^n$ be polynomials with integer coefficients, of degrees $m\geq 2$ and $n\geq 2$, with $a_0\neq 0$ and $|b_n|=1$. Assume that $|a_m|=p^k$, where p is a prime number and k is coprime to mn. If*

$$p>(|a_0|+|a_1|+\cdots+|a_{m-1}|)^{\max\{m,n\}-1},$$

then the polynomial $f\circ g$ is irreducible over $\mathbb{Q}$.

We note that the conditions on p in the statements of the results above do not depend on $b_0,b_1,\dots,b_{n-1}$, so the conclusion on the irreducibility of $f\circ g$ will hold once we choose $a_0,\dots,a_{m-1}$, b_n and p to satisfy the inequalities in the statements of Theorems 1, 2 and 3, respectively, then choose a suitable k, and let $b_0,b_1,\dots,b_{n-1}$ vary independently. We also note that in the results above we can not drop the arithmetical condition on k and solely ask p to be sufficiently large. To see this, consider the polynomial $f(X)=p^pX^p-1$, with p a prime number. In this case, $a_p=p^p$ and $k=\deg f=p$, so we cannot apply Corollary 3; in fact, f is obviously reducible, being divisible by $pX-1$. Besides, in our results the condition on the magnitude of p implies that the leading coefficient of g is not divisible by p. For an example where the conclusion on the irreducibility of $f\circ g$ fails if we allow b_n to be divisible by p, let us consider an irreducible polynomial $f(X)$ with integer coefficients, of degree $m \geq 2$, having leading coefficient $a_m = p^k q$ with p prime, q an integer not divisible by p, and k a positive integer coprime to m (such polynomials do exist, according to Corollary 3, for instance). Let $g(X) = f(X) + X$, so $m = n$ and $a_m = b_n$, and let θ be a root of f. Since $f(g(\theta)) = f(f(\theta) + \theta) = f(\theta) = 0$, we deduce that $f \circ g$ is reducible over $\mathbb{Q}$, being divisible by f, and this holds for an arbitrary choice of the prime p.

We will first prove Theorem 1, and then we will adapt its proof to the case that f is known to be irreducible, when we can make use of the crucial information on the degrees of the hypothetical factors of $f \circ g$ provided by Capelli's Theorem. This will allow us to relax the conditions on k and on the magnitude of p, as in Theorem 2.

Proof of Theorem 1. First of all, we note that $f \circ g$ is irreducible for $m = n = 1$, without any restriction on k or p, since it is linear. Therefore in what follows we will assume that $mn > 1$. By our assumption on p we see in particular that $p > |q|$ and $p > |b_n|$, so $p \nmid qb_n$. Now let us assume to the contrary that $f(g(X))$ is reducible, say

$$f(g(X)) = F_1(X)F_2(X)$$

with $F_1, F_2 \in \mathbb{Z}[X]$, $\deg F_1 \geq 1, \deg F_2 \geq 1$, and let t_1 and t_2 be the leading coefficients of F_1 and F_2 respectively. Then, by comparing the leading coefficients in this equality we obtain

$$t_1 t_2 = a_m b_n^m = p^k q b_n^m. \tag{2.1}$$

Let us now write $t_1 = p^\alpha t_1'$ and $t_2 = p^\beta t_2'$ with α, β non-negative integers and $t_1', t_2' \in \mathbb{Z}$, $p \nmid t_1' t_2'$. By (2.1) and the fact that $p \nmid qb_n$ we must have

$$\alpha + \beta = k \tag{2.2}$$

and

$$t_1' t_2' = q b_n^m. \tag{2.3}$$

We note that we may also write $f(g(X)) = h(X) + p^k q \cdot g^m(X)$, with

$$h(X) = a_0 + a_1 g(X) + \cdots + a_{m-1} g^{m-1}(X).$$

Now, since $a_0 \neq 0$, we deduce that $h(X)$ and $g^m(X)$ are algebraically relatively prime (i.e. they can only share a constant factor), so the same must hold for $g^m(X)$ and $F_1(X)$, and also for $g^m(X)$ and $F_2(X)$. As a consequence, the resultants $R(g^m, F_1)$ and $R(g^m, F_2)$ must be nonzero rational integers, so we must have

$$|R(g^m, F_1)| \geq 1 \quad \text{and} \quad |R(g^m, F_2)| \geq 1. \tag{2.4}$$

In the remainder of the proof, we will estimate $|R(g^m, F_1)|$ and $|R(g^m, F_2)|$ in a different way. If we consider the factorizations of $F_1(X)$ and $F_2(X)$ over $\mathbb{C}$, say

$$F_1(X) = t_1(X - \alpha_1) \cdots (X - \alpha_r) \quad \text{and} \quad F_2(X) = t_2(X - \beta_1) \cdots (X - \beta_s)$$

with $\alpha_1, \ldots, \alpha_r, \beta_1, \ldots, \beta_s \in \mathbb{C}$, $r, s \geq 1$ and $r + s = mn$, then we have

$$|R(g^m, F_1)| = |t_1|^{mn} \prod_{1 \leq j \leq r} |g^m(\alpha_j)| \quad \text{and} \quad |R(g^m, F_2)| = |t_2|^{mn} \prod_{1 \leq j \leq s} |g^m(\beta_j)|. \tag{2.5}$$

We note that since g and h are relatively prime, we have $g(\alpha_j) \neq 0$, $h(\alpha_j) \neq 0$ and also $g(\beta_j) \neq 0$, $h(\beta_j) \neq 0$. All that remains now is to prove that our assumption on the magnitude of p actually forces one of the inequalities $|R(g^m, F_1)| < 1$ and $|R(g^m, F_2)| < 1$ to hold, which contradicts (2.4). To do this, we need to find upper bounds for the absolute values of the two resultants in (2.5). We first observe that since $f(g(\alpha_j)) = 0$ for $1 \leq j \leq r$ and $f(g(\beta_j)) = 0$ for $1 \leq j \leq s$, we have

$$|g^m(\alpha_j)| = \frac{|h(\alpha_j)|}{|a_m|},\ 1 \leq j \leq r, \quad \text{and} \quad |g^m(\beta_j)| = \frac{|h(\beta_j)|}{|a_m|},\ 1 \leq j \leq s,$$

so instead of (2.5) we may write

$$|R(g^m, F_1)| = p^{\alpha mn - kr} |t_1'|^{mn} \prod_{1 \leq j \leq r} \frac{|h(\alpha_j)|}{|q|} \tag{2.6}$$

and

$$|R(g^m, F_2)| = p^{\beta mn - ks} |t_2'|^{mn} \prod_{1 \leq j \leq s} \frac{|h(\beta_j)|}{|q|}. \tag{2.7}$$

We now analyze the exponents $\alpha mn - kr$ and $\beta mn - ks$ of the prime p appearing in (2.6) and (2.7), respectively. To do this we will adapt an idea from [13], and use our key assumption that k and mn are coprime. Using (2.2) and the fact that $r + s = mn$, we observe that

$$(\alpha mn - kr) + (\beta mn - ks) = mn(\alpha + \beta) - k(r + s) = mnk - kmn = 0. \tag{2.8}$$

Assume now without loss of generality that $\alpha mn - kr \leq \beta mn - ks$. We will prove that neither $\alpha mn - kr$, nor $\beta mn - ks$ can be zero. As these two integers sum up to zero, if one of them is zero, the other one must be zero too. So let us suppose that $\alpha mn = kr$ and $\beta mn = ks$. As k and mn are coprime, these equalities force both r and s to be divisible by mn, and since $r + s = mn$, this would imply that one of r and s must be zero, a contradiction. Therefore, there exists a positive integer δ such that $\alpha mn - kr = -\delta$ and $\beta mn - ks = \delta$. In particular, by (2.6) and (2.3) we deduce that

$$|R(g^m, F_1)| = \frac{|t_1'|^{mn}}{p^\delta} \prod_{1 \leq j \leq r} \frac{|h(\alpha_j)|}{|q|} \leq \frac{|qb_n^m|^{mn}}{p^\delta} \prod_{1 \leq j \leq r} \frac{|h(\alpha_j)|}{|q|}. \tag{2.9}$$

In what follows, we will find an upper bound for $|h(\alpha_j)|$, $1 \leq j \leq r$. To this end, we will actually need to find first an upper bound for $g(\alpha_j)$, $1 \leq j \leq r$, which in turn will require an upper bound for the roots of f. So let us consider the factorization of $f(X)$, say

$$f(X) = a_m(X - \theta_1) \cdots (X - \theta_m),$$

with $\theta_1, \ldots, \theta_m \in \mathbb{C}$.

Let us first assume that $|a_0| \geq |q|$, so $\lambda = (|b_n|^{mnk} |a_0|^{\frac{(mn-1)k-1}{m}} |q|^{\frac{k+1}{m}})^{-1}$. Our assumption on the magnitude of p implies in particular that $p > |b_n|^{m^2 n} |q| L^*(f(\lambda X))^{mn-1}$, so

$$\begin{aligned} p^k |q| &> |b_n|^{m^2 nk} |q|^{k+1} L^*(f(\lambda X))^{(mn-1)k} \\ &= [\lambda^m |b_n|^{m^2 nk} |q|^{k+1} L^*(f(\lambda X))^{(mn-1)k-1}] \cdot (|a_0| \lambda^{-m} + \cdots + |a_{m-1}| \lambda^{-1}). \end{aligned}$$

The quantity in square brackets above is equal to

$$\left(\frac{L^*(f(\lambda X))}{|a_0|}\right)^{(mn-1)k-1},$$

which is at least 1, since $|a_0| \leq L^*(f(\lambda X))$ and $(mn-1)k-1 \geq 0$ (as $mn \geq 2$).

Assume now that $|a_0| < |q|$, so $\lambda = (|b_n|^{mnk}|a_0|^{\frac{k-1}{m}}|q|^{\frac{(mn-1)k+1}{m}})^{-1}$. Our assumption on the magnitude of p also implies that $p > |b_n|^{m^2n}|q|^{mn-1}L^*(f(\lambda X))$, so

$$\begin{aligned} p^k|q| &> |b_n|^{m^2nk}|q|^{(mn-1)k+1}L^*(f(\lambda X))^k \\ &= [\lambda^m|b_n|^{m^2nk}|q|^{(mn-1)k+1}L^*(f(\lambda X))^{k-1}] \cdot (|a_0|\lambda^{-m} + \cdots + |a_{m-1}|\lambda^{-1}). \end{aligned}$$

Here the quantity in square brackets above is equal to

$$\left(\frac{L^*(f(\lambda X))}{|a_0|}\right)^{k-1},$$

which is still at least 1, as $k \geq 1$.

We have thus proved that in each of these two cases we have

$$p^k|q| > |a_0|\lambda^{-m} + \cdots + |a_{m-1}|\lambda^{-1}.$$

It is a standard fact that this condition forces all the roots $\theta_1, \ldots, \theta_m$ of f to lie in the open disk $\{|z| < \lambda\}$. This is an immediate consequence of Rouché's Theorem, but can also be checked in an elementary way, for if f had a root θ with $|\theta| \geq \lambda$, then we would obtain

$$0 = \left|\sum_{i=0}^{m} a_i\theta^{i-m}\right| \geq p^k|q| - \sum_{i=0}^{m-1}|a_i| \cdot |\theta|^{i-m} \geq p^k|q| - (|a_0|\lambda^{-m} + \cdots + |a_{m-1}|\lambda^{-1}) > 0,$$

a contradiction. Therefore, for any $i \in \{1, \ldots, m\}$ one has

$$|\theta_i| < \lambda. \tag{2.10}$$

Let us fix now an index $j \in \{1, \ldots, r\}$ and recall that $f(g(\alpha_j)) = 0$. Therefore there exists an index $i \in \{1, \ldots, m\}$, depending on j, for which $g(\alpha_j) = \theta_i$, which in view of (2.10) shows that we must have

$$|g(\alpha_j)| < \lambda, \tag{2.11}$$

uniformly, for each $j = 1, \ldots, r$. Recalling the definition of $h(X)$, one deduces by (2.11) that $|h(\alpha_j)| < |a_0| + |a_1|\lambda + \cdots + |a_{m-1}|\lambda^{m-1}$, that is $|h(\alpha_j)| < L^*(f(\lambda X))$, uniformly, for each $j = 1, \ldots, r$, which in view of (2.9) yields

$$|R(g^m, F_1)| \leq \frac{|q|^{mn}|b_n|^{m^2n}}{p^\delta} \cdot \left(\frac{L^*(f(\lambda X))}{|q|}\right)^r. \tag{2.12}$$

We distinguish now two cases:

Case 1: $|q| > L^*(f(\lambda X))$. In this case, as $\delta \geq 1$ and $r \geq 1$, we deduce by (2.12) that

$$|R(g^m, F_1)| \leq \frac{1}{p} \cdot |q|^{mn-1}|b_n|^{m^2n}L^*(f(\lambda X)),$$

which gives the desired contradiction $|R(g^m,F_1)|<1$ if $p>|q|^{mn-1}|b_n|^{m^2n}L^*(f(\lambda X))$.

Case 2: $|q|\leq L^*(f(\lambda X))$. In this second case, as $\delta\geq 1$ and $r\leq mn-1$, we deduce by (2.12) that

$$\begin{aligned}|R(g^m,F_1)| &\leq \frac{|q|^{mn}|b_n|^{m^2n}}{p}\cdot\left(\frac{L^*(f(\lambda X))}{|q|}\right)^{mn-1}\\ &= \frac{1}{p}\cdot|q|\cdot|b_n|^{m^2n}L^*(f(\lambda X))^{mn-1},\end{aligned}$$

which gives the desired contradiction if $p>|q|\cdot|b_n|^{m^2n}L^*(f(\lambda X))^{mn-1}$. Summarizing, we conclude that $|R(g^m,F_1)|<1$ if

$$p>|b_n|^{m^2n}\cdot\min\{|q|,L^*(f(\lambda X))\}\cdot\max\{|q|,L^*(f(\lambda X))\}^{mn-1},$$

which is precisely the condition on the magnitude of p in the statement of our theorem. So if p satisfies this inequality, the polynomial $f(g(X))$ (and hence $f(X)$ too) must be irreducible over $\mathbb{Q}$, which completes the proof of the theorem. □

Proof of Corollary 2. Since $|a_0qb_n|>1$, we have $\lim\limits_{k\to\infty}\lambda=0$, so $\lim\limits_{k\to\infty}L^*(f(\lambda X))=|a_0|$, which in turn shows that

$$\lim_{k\to\infty}|b_n|^{m^2n}\cdot\min\{|q|,L^*(f(\lambda X))\}\cdot\max\{|q|,L^*(f(\lambda X))\}^{mn-1}=$$
$$|b_n|^{m^2n}\cdot\min\{|q|,|a_0|\}\cdot\max\{|q|,|a_0|\}^{mn-1}.$$

Since $p>|b_n|^{m^2n}\cdot\min\{|q|,|a_0|\}\cdot\max\{|q|,|a_0|\}^{mn-1}$, for sufficiently large k we will have

$$p>|b_n|^{m^2n}\cdot\min\{|q|,L^*(f(\lambda X))\}\cdot\max\{|q|,L^*(f(\lambda X))\}^{mn-1}.$$

Thus, for sufficiently large integers k that are coprime to mn, we may apply Theorem 1 to conclude that the polynomial $f\circ g$ is irreducible over $\mathbb{Q}$. □

Proof of Corollary 3. The result follows by Theorem 1 with $n=b_n=1$. □

Proof of Corollary 4. Our assumption that $|q|>|a_0|$ implies that λ in Corollary 3 is equal to $|a_0|^{-\frac{k-1}{m}}|q|^{-\frac{(m-1)k+1}{m}}$, so

$$\begin{aligned}L^*(f(\lambda X)) &= |a_0|+\frac{|a_1|}{|a_0|^{\frac{k-1}{m}}|q|^{\frac{(m-1)k+1}{m}}}+\cdots+\frac{|a_{m-1}|}{|a_0|^{\frac{k-1}{m}(m-1)}|q|^{\frac{(m-1)k+1}{m}(m-1)}}\\ &\leq |a_0|+\frac{|a_1|+\cdots+|a_{m-1}|}{|a_0|^{\frac{k-1}{m}}|q|^{\frac{(m-1)k+1}{m}}}<|a_0|+1.\end{aligned}$$

Last inequality above is equivalent to $k>\log_{|a_0|^{\frac{1}{m}}|q|^{\frac{m-1}{m}}}A$, with

$$A:=(|a_1|+\cdots+|a_{m-1}|)\cdot\frac{|a_0|^{\frac{1}{m}}}{|q|^{\frac{1}{m}}},$$

which holds true, according to our assumption that

$$k > \log_{|a_0|^{\frac{1}{m}}|q|^{\frac{m-1}{m}}}(|a_1| + \cdots + |a_{m-1}|),$$

together with the fact that $|a_0|^{\frac{1}{m}} < |q|^{\frac{1}{m}}$.

On the other hand, since $|q| \geq |a_0| + 1 > L^*(f(\lambda X))$ and $p > (1 + |a_0|)|q|^{m-1}$, the condition $p > \min\{|q|, L^*(f(\lambda X))\} \cdot \max\{|q|, L^*(f(\lambda X))\}^{m-1}$ in Corollary 3 is fulfilled, so f must be irreducible over $\mathbb{Q}$. □

Proof of Corollary 5. Here our assumption that $|q| \leq |a_0|$ implies that λ in Corollary 3 is equal to $|a_0|^{-\frac{(m-1)k-1}{m}}|q|^{-\frac{(k+1)}{m}}$, so

$$\begin{aligned} L^*(f(\lambda X)) &= |a_0| + \frac{|a_1|}{|a_0|^{\frac{(m-1)k-1}{m}}|q|^{\frac{k+1}{m}}} + \cdots + \frac{|a_{m-1}|}{|a_0|^{\frac{(m-1)k-1}{m}(m-1)}|q|^{\frac{k+1}{m}(m-1)}} \\ &\leq |a_0| + \frac{|a_1| + \cdots + |a_{m-1}|}{|a_0|^{\frac{(m-1)k-1}{m}}|q|^{\frac{k+1}{m}}} < |a_0| + 1. \end{aligned}$$

The right-most inequality above is equivalent to $k > \log_{|a_0|^{\frac{m-1}{m}}|q|^{\frac{1}{m}}} A$, with

$$A := (|a_1| + \cdots + |a_{m-1}|) \cdot \frac{|a_0|^{\frac{1}{m}}}{|q|^{\frac{1}{m}}},$$

which obviously holds, according to our assumption that

$$k > 1 + \log_{|a_0|^{\frac{m-1}{m}}|q|^{\frac{1}{m}}}(|a_1| + \cdots + |a_{m-1}|),$$

and to the fact that $|a_0|^{\frac{m-1}{m}}|q|^{\frac{1}{m}} \geq |a_0/q|^{\frac{1}{m}}$, as $|q| \leq |a_0|$.

Next, as $|a_0| + 1 > L^*(f(\lambda X)) \geq |a_0| \geq |q|$ and $p > (1 + |a_0|)^{m-1}|q|$, we conclude that the condition $p > \min\{|q|, L^*(f(\lambda X))\} \cdot \max\{|q|, L^*(f(\lambda X))\}^{m-1}$ in Corollary 3 is satisfied, which proves the irreducibility of f. □

Proof of Theorem 2. Here we know that f is irreducible over $\mathbb{Q}$, so obviously $f(b_0 + b_1 X)$ must also be irreducible over $\mathbb{Q}$ for every $b_0, b_1 \in \mathbb{Z}$ with $b_1 \neq 0$. We may therefore assume that $n > 1$, so by our assumption on p we can deduce in this case too that $p > |b_n|$ and $p > |q|$, hence $p \nmid qb_n$. The proof continues as in the case of Theorem 1, with the main differences coming from the important information on the degrees of F_1 and F_2 given by Capelli's Theorem. More precisely, as f is known to be irreducible, the degree of every irreducible factor of $f(g(X))$ must be a multiple of m, which implies in particular that $\deg F_1 = r \geq m$ and also $\deg F_2 = s \geq m$. Therefore here we may conclude that

$$m \leq r, s \leq mn - m. \tag{2.13}$$

Besides, when we try as before to prove that none of the integers $\alpha mn - kr$ and $\beta mn - ks$ can be zero, it suffices to only ask k to be coprime to n (instead of mn as in Theorem 1), and this too is due to the fact that r and s are both multiples of m. Indeed, as $r = mr'$

and $s = ms'$ for some integers r' and s', if we assume that $\alpha mn = kr$ and $\beta mn = ks$, we obtain

$$\alpha n = kr' \quad \text{and} \quad \beta n = ks'.$$

As k is coprime to n, these equalities will force both r' and s' to be divisible by n, which in turn will force both r and s to be divisible by mn. Since $r + s = mn$, this will further imply that one of r and s must be zero, a contradiction.

Last, but not least, we notice that in this case the non-zero integers $\alpha mn - kr$ and $\beta mn - ks$ are both multiples of m, hence δ is a positive multiple of m, so in particular we have

$$\delta \geq m. \tag{2.14}$$

Let us first assume that $|a_0| \geq |q|$, so $\lambda = (|b_n|^{nk}|a_0|^{\frac{(n-1)k-1}{m}}|q|^{\frac{k+1}{m}})^{-1}$. Our assumption on the magnitude of p implies in particular that $p > |b_n|^{mn}|q|L^*(f(\lambda X))^{n-1}$, so

$$\begin{aligned} p^k|q| &> |b_n|^{mnk}|q|^{k+1}L^*(f(\lambda X))^{(n-1)k} \\ &= [\lambda^m|b_n|^{mnk}|q|^{k+1}L^*(f(\lambda X))^{(n-1)k-1}] \cdot (|a_0|\lambda^{-m} + \cdots + |a_{m-1}|\lambda^{-1}). \end{aligned}$$

The quantity in square brackets above is equal to

$$\left(\frac{L^*(f(\lambda X))}{|a_0|}\right)^{(n-1)k-1},$$

which is at least 1, since $|a_0| \leq L^*(f(\lambda X))$ and $(n-1)k - 1 \geq 0$ (as $n > 1$).

Assume next that $|a_0| < |q|$, so $\lambda = (|b_n|^{nk}|a_0|^{\frac{k-1}{m}}|q|^{\frac{(n-1)k+1}{m}})^{-1}$. Our assumption on the magnitude of p also implies that $p > |b_n|^{mn}|q|^{n-1}L^*(f(\lambda X))$, so

$$\begin{aligned} p^k|q| &> |b_n|^{mnk}|q|^{(n-1)k+1}L^*(f(\lambda X))^{k} \\ &= [\lambda^m|b_n|^{mnk}|q|^{(n-1)k+1}L^*(f(\lambda X))^{k-1}] \cdot (|a_0|\lambda^{-m} + \cdots + |a_{m-1}|\lambda^{-1}). \end{aligned}$$

Here the quantity in square brackets above is equal to

$$\left(\frac{L^*(f(\lambda X))}{|a_0|}\right)^{k-1},$$

which is still at least 1, as $k \geq 1$.

We thus proved that in this case too we have

$$p^k|q| > |a_0|\lambda^{-m} + \cdots + |a_{m-1}|\lambda^{-1},$$

so we may still conclude that all the roots $\theta_1, \ldots, \theta_m$ of f lie in the open disk $\{|z| < \lambda\}$.

Here too we will analyze separately the cases that $|q|$ exceeds or not $L^*(f(\lambda X))$:

Case 1: $|q| > L^*(f(\lambda X))$. In this case, since $r \geq m$ and $\delta \geq m$ (according to (2.14)), we deduce by (2.12) that

$$|R(g^m, F_1)| \leq \frac{|q|^{mn}|b_n|^{m^2n}}{p^m} \cdot \left(\frac{L^*(f(\lambda X))}{|q|}\right)^m,$$

which gives the desired contradiction $|R(g^m, F_1)| < 1$ if $p > |q|^{n-1}|b_n|^{mn}L^*(f(\lambda X))$.

Case 2: $|q| \leq L^*(f(\lambda X))$. Here, since by (2.13) we have $r \leq mn - m$, we deduce by (2.14) and (2.12) that

$$\begin{aligned} |R(g^m, F_1)| &\leq \frac{|q|^{mn}|b_n|^{m^2n}}{p^m} \cdot \left(\frac{L^*(f(\lambda X))}{|q|}\right)^{mn-m} \\ &= \frac{|q|^m \cdot |b_n|^{m^2n}(L^*(f(\lambda X)))^{mn-m}}{p^m}, \end{aligned}$$

which gives the desired contradiction $|R(g^m, F_1)| < 1$ if $p > |q| \cdot |b_n|^{mn} L^*(f(\lambda X))^{n-1}$. We conclude that $|R(g^m, F_1)| < 1$ in each of these two cases if

$$p > |b_n|^{mn} \cdot \min\{|q|, L^*(f(\lambda X))\} \cdot \max\{|q|, L^*(f(\lambda X))\}^{n-1},$$

so if p satisfies this inequality, the polynomial $f \circ g$ (and hence f too) must be irreducible over $\mathbb{Q}$. □

Proof of Corollary 6. Since $|b_n| = 1$ and $m = n$ we see that

$$\lambda_1 = \lambda_2 = (|a_0|^{\frac{k-1}{m}} |q|^{\frac{k+1}{m}} \cdot \max\{|a_0|, |q|\}^{\frac{(m-2)k}{m}})^{-1}, \tag{2.15}$$

and the condition on p in Theorem 3 reduces to

$$p > \min\{|q|, L^*(f(\lambda X))\} \cdot \max\{|q|, L^*(f(\lambda X))\}^{m-1},$$

with λ given by (2.15). The conclusion follows now by Theorem 3. □

Proof of Corollary 7. In this case, as $m \geq 2$ and $n \geq 2$, both λ_1 and λ_2 are at most 1, so it suffices to ask p to satisfy $p > (|a_0| + |a_1| + \cdots + |a_{m-1}|)^{\max\{m,n\}-1}$. □

3 The case that the inverse of k modulo mn is known

As seen in the proof of the results in the previous section, there is an intimate connection between the arithmetical properties of k and the possible degrees of the hypothetical factors of $f \circ g$. In this section we will provide some sharper irreducibility conditions for the case that some additional information on k is known. More precisely, we will present some refinements of the lower bounds on p in the case that the inverse of k modulo mn (or modulo n) is known.

Our first result that uses information on the inverse of k modulo mn is the following.

Theorem 4. *Let $f(X) = a_0 + \cdots + a_m X^m$ and $g(X) = b_0 + \cdots + b_n X^n$ be non-constant polynomials with integer coefficients, with $a_0 a_m b_n \neq 0$. Assume that $a_m = p^k q$ with p a prime number, q an integer, and k a positive integer coprime to mn. Let $\ell \in \{1, \ldots, mn-1\}$ be the inverse of k modulo mn, and let $\lambda = (|q|^{\frac{(mn-\ell)k+1}{m}} |a_0|^{\frac{\ell k-1}{m}} |b_n|^{mnk})^{-1}$. If*

$$\begin{aligned} p > \max\Big\{&|q|^{mn-\ell}|b_n|^{m^2n} L^*(f(\lambda X))^{\ell}, |q|^{\frac{mn-1}{2}} |b_n|^{\frac{m^2n}{2}} L^*(f(\lambda X))^{\frac{1}{2}}, \\ &|q|^{\frac{1}{2}} |b_n|^{\frac{m^2n}{2}} L^*(f(\lambda X))^{\frac{mn-1}{2}}\Big\}, \end{aligned}$$

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

Remark 1. *As we shall see in the proof of Theorem 4, if* $k > 1$*, or if* $k = 1$ *and* $mn \geq 3$*, we may slightly decrease the value of* λ *above by replacing it with*

$$\lambda' = \max\{|q|^{\frac{(mn-\ell)k+1}{m}}|a_0|^{\frac{\ell k-1}{m}}|b_n|^{mnk}, |q|^{\frac{k+2}{2m}}|a_0|^{\frac{(mn-1)k-2}{2m}}|b_n|^{\frac{mnk}{2}}\}^{-1}.$$

Moreover, if $k > 1$ *we may further decrease the value of* λ *to*

$$\begin{aligned}\lambda'' \quad = \quad & \max\{|q|^{\frac{(mn-\ell)k+1}{m}}|a_0|^{\frac{\ell k-1}{m}}|b_n|^{mnk}, |q|^{\frac{k+2}{2m}}|a_0|^{\frac{(mn-1)k-2}{2m}}|b_n|^{\frac{mnk}{2}},\\ & |q|^{\frac{(mn-1)k+2}{2m}}|a_0|^{\frac{k-2}{2m}}|b_n|^{\frac{mnk}{2}}\}^{-1}.\end{aligned}$$

In particular, for $g(X) = X$ one obtains the following irreducibility criterion.

Corollary 8. *Let* $f(X) = a_0 + a_1X + \cdots + a_mX^m$ *be a non-constant polynomial with integer coefficients, with* $a_0 \neq 0$*. Assume that* $a_m = p^kq$ *with* p *a prime number,* q *a non-zero integer, and* k *a positive integer coprime to* m*. Let* $\ell \in \{1, \ldots, m-1\}$ *be the inverse of* k *modulo* m*, and let* $\lambda = (|q|^{\frac{(m-\ell)k+1}{m}}|a_0|^{\frac{\ell k-1}{m}})^{-1}$*. If*

$$p > \max\left\{|q|^{m-\ell}L^*(f(\lambda X))^{\ell},\ |q|^{\frac{m-1}{2}}L^*(f(\lambda X))^{\frac{1}{2}},\ |q|^{\frac{1}{2}}L^*(f(\lambda X))^{\frac{m-1}{2}}\right\},$$

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

According to Remark 1, if $k > 1$, or if $k = 1$ and $m \geq 3$, we may slightly decrease the value of λ in Corollary 8 by replacing it with

$$\lambda' = \max\left\{|q|^{\frac{(m-\ell)k+1}{m}}|a_0|^{\frac{\ell k-1}{m}}, |q|^{\frac{k+2}{2m}}|a_0|^{\frac{(m-1)k-2}{2m}}\right\}^{-1}.$$

Moreover, if $k > 1$ we may further decrease the value of λ to

$$\lambda'' = \max\left\{|q|^{\frac{(m-\ell)k+1}{m}}|a_0|^{\frac{\ell k-1}{m}}, |q|^{\frac{k+2}{2m}}|a_0|^{\frac{(m-1)k-2}{2m}}, |q|^{\frac{(m-1)k+2}{2m}}|a_0|^{\frac{k-2}{2m}}\right\}^{-1}.$$

One may obtain some simpler irreducibility conditions in the case that $|q| = 1$ and $k \equiv 1 \pmod{m}$, or $k \equiv 2 \pmod{m}$, as in the following two results.

Corollary 9. *Let* $f(X) = a_0 + a_1X + \cdots + a_mX^m$ *be a polynomial with integer coefficients, of degree* $m \geq 3$*,* $a_0 \neq 0$*. If* $a_m = p^k$*, where* p *is a prime number,* $k \equiv 1 \pmod{m}$*, and* $p > (|a_0| + \cdots + |a_{m-1}|)^{\frac{m-1}{2}}$*, then* f *is irreducible over* $\mathbb{Q}$*.*

Corollary 10. *Let* $f(X) = a_0 + a_1X + \cdots + a_mX^m$ *be a polynomial with integer coefficients, of odd degree* m*,* $a_0 \neq 0$*. If* $a_m = p^k$*, where* p *is a prime number,* $k \equiv 2 \pmod{m}$*, and* $p > (|a_0| + \cdots + |a_{m-1}|)^{\frac{m+1}{2}}$*, then* f *is irreducible over* $\mathbb{Q}$*.*

As in previous section, we can relax the restrictions on p and k in the case that f is known to be irreducible.

Theorem 5. *Let* $f(X) = a_0 + \cdots + a_mX^m$ *and* $g(X) = b_0 + \cdots + b_nX^n$ *be non-constant polynomials with integer coefficients,* $a_0a_mb_n \neq 0$*,* f *irreducible over* $\mathbb{Q}$*. Assume* $a_m = p^kq$

with p prime, q an integer, and k a positive integer coprime to n. Let $\ell \in \{1, \dots, n-1\}$ be the inverse of k modulo n, and let $\lambda = (|q|^{\frac{(n-\ell)k+1}{m}} |a_0|^{\frac{\ell k-1}{m}} |b_n|^{nk})^{-1}$. If

$$p > \max\Big\{ |q|^{n-\ell} |b_n|^{mn} L^*(f(\lambda X))^{\ell}, |q|^{\frac{n-1}{2}} |b_n|^{\frac{mn}{2}} L^*(f(\lambda X))^{\frac{1}{2}}, \\ |q|^{\frac{1}{2}} |b_n|^{\frac{mn}{2}} L^*(f(\lambda X))^{\frac{n-1}{2}} \Big\},$$

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

Remark 2. *We mention that if $n \geq 2$ and $k \geq 2$, or if $n \geq 3$ and $k = 1$, we may decrease the value of λ in Theorem 5 by replacing it with*

$$\lambda' = \max\Big\{ |q|^{\frac{(n-\ell)k+1}{m}} |a_0|^{\frac{\ell k-1}{m}} |b_n|^{nk}, |q|^{\frac{k+2}{2m}} |a_0|^{\frac{(n-1)k-2}{2m}} |b_n|^{\frac{nk}{2}} \Big\}^{-1}.$$

Moreover, if $k \geq 2$ we may further decrease the value of λ to

$$\lambda'' = \max\Big\{ |q|^{\frac{(n-\ell)k+1}{m}} |a_0|^{\frac{\ell k-1}{m}} |b_n|^{nk}, |q|^{\frac{k+2}{2m}} |a_0|^{\frac{(n-1)k-2}{2m}} |b_n|^{\frac{nk}{2}}, |q|^{\frac{(n-1)k+2}{2m}} |a_0|^{\frac{k-2}{2m}} |b_n|^{\frac{nk}{2}} \Big\}^{-1}.$$

We may obviously drop the condition that f is irreducible over $\mathbb{Q}$ by combining Corollary 8 and Theorem 5. In this respect we will only present here a simple example where the irreducibility conditions drastically simplify, namely the case that $|q| = |b_n| = 1$ and k satisfies the congruences $k \equiv 1 \pmod m$ and $k \equiv 1 \pmod n$.

Corollary 11. *Let $f(X) = a_0 + \cdots + a_m X^m$ and $g(X) = b_0 + \cdots + b_n X^n$ be polynomials with integer coefficients, of degrees $m \geq 3$ and $n \geq 3$, with $a_0 \neq 0$ and $|b_n| = 1$. Assume that $a_m = p^k$, where p is a prime number and k satisfies $k \equiv 1 \pmod m$ and $k \equiv 1 \pmod n$. If*

$$p > (|a_0| + |a_1| + \cdots + |a_{m-1}|)^{\frac{\max\{m,n\}-1}{2}},$$

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

Proof of Theorem 4. Here too the assumption on p implies that both q and b_n are not divisible by p. The proof continues as in the case of Theorem 1. Our assumption on the magnitude of p implies that $p > |q|^{mn-\ell} |b_n|^{m^2 n} L^*(f(\lambda X))^{\ell}$, so

$$\begin{aligned} p^k |q| &> |q|^{(mn-\ell)k+1} |b_n|^{m^2 nk} L^*(f(\lambda X))^{\ell k} \\ &= [\lambda^m |q|^{(mn-\ell)k+1} |b_n|^{m^2 nk} L^*(f(\lambda X))^{\ell k-1}] \cdot (|a_0| \lambda^{-m} + \cdots + |a_{m-1}| \lambda^{-1}). \end{aligned}$$

Recalling that $\lambda = (|q|^{\frac{(mn-\ell)k+1}{m}} |a_0|^{\frac{\ell k-1}{m}} |b_n|^{mnk})^{-1}$, we deduce that the quantity in the square brackets above is equal to

$$\left(\frac{L^*(f(\lambda X))}{|a_0|} \right)^{\ell k-1},$$

which is at least 1, as $L^*(f(\lambda X)) \geq |a_0|$, and the exponent $\ell k - 1$ is nonnegative.

We will consider now the situation mentioned in Remark 1. So let us assume now that

$$\lambda = (|q|^{\frac{k+2}{2m}} |a_0|^{\frac{(mn-1)k-2}{2m}} |b_n|^{\frac{mnk}{2}})^{-1}.$$

The hypothesis on the magnitude of p also implies that $p>|q|^{\frac{1}{2}}|b_n|^{\frac{m^2n}{2}}L^*(f(\lambda X))^{\frac{mn-1}{2}}$, so

$$\begin{aligned}p^k|q| &> |q|^{\frac{k}{2}+1}|b_n|^{\frac{m^2nk}{2}}L^*(f(\lambda X))^{\frac{(mn-1)k}{2}}\\ &= [\lambda^m|q|^{\frac{k}{2}+1}|b_n|^{\frac{m^2nk}{2}}L^*(f(\lambda X))^{\frac{(mn-1)k}{2}-1}]\cdot(|a_0|\lambda^{-m}+\cdots+|a_{m-1}|\lambda^{-1}).\end{aligned}$$

Observe that the quantity in the square brackets above is this time equal to

$$\left(\frac{L^*(f(\lambda X))}{|a_0|}\right)^{\frac{(mn-1)k}{2}-1},$$

which is at least 1 if the exponent $\frac{(mn-1)k}{2}-1$ is nonnegative. This last condition obviously holds if $mn\geq 3$, as $k\geq 1$, but also holds for $mn=2$, provided $k\geq 2$ (the irreducibility of $f\circ g$ in the case that both m and n are equal to 1 is trivial).

Finally, let us assume that

$$\lambda=(|q|^{\frac{(mn-1)k+2}{2m}}|a_0|^{\frac{k-2}{2m}}|b_n|^{\frac{mnk}{2}})^{-1}.$$

Since our assumption on the magnitude of p implies that $p>|q|^{\frac{mn-1}{2}}|b_n|^{\frac{m^2n}{2}}L^*(f(\lambda X))^{\frac{1}{2}}$, we deduce that

$$\begin{aligned}p^k|q| &> |q|^{\frac{(mn-1)k+2}{2}}|b_n|^{\frac{m^2nk}{2}}L^*(f(\lambda X))^{\frac{k}{2}}\\ &= [\lambda^m|q|^{\frac{(mn-1)k+2}{2}}|b_n|^{\frac{m^2nk}{2}}L^*(f(\lambda X))^{\frac{k}{2}-1}]\cdot(|a_0|\lambda^{-m}+\cdots+|a_{m-1}|\lambda^{-1}).\end{aligned}$$

Observe that the quantity in the square brackets above is equal to

$$\left(\frac{L^*(f(\lambda X))}{|a_0|}\right)^{\frac{k}{2}-1},$$

which is at least 1 for $k\geq 2$.

We have thus checked that in each of the above three cases we have

$$p^k|q|>|a_0|\lambda^{-m}+\cdots+|a_{m-1}|\lambda^{-1}.$$

We may therefore still conclude that all the roots $\theta_1,\ldots,\theta_m$ of f lie in the open disk $\{|z|<\lambda\}$, and then deduce that

$$|R(g^m,F_1)|\leq\frac{|q|^{mn}|b_n|^{m^2n}}{p^\delta}\cdot\left(\frac{L^*(f(\lambda X))}{|q|}\right)^r. \tag{3.1}$$

We distinguish now three cases:

Case 1: $\delta=1$. Observe now that if $\delta=1$, then by reducing modulo mn the equality $\alpha mn-kr=-1$ we obtain $kr\equiv 1 \pmod{mn}$, and since $r\in\{1,\ldots,mn-1\}$, we must have $r=\ell$. In this case we deduce by (3.1) that

$$|R(g^m,F_1)|\leq\frac{|q|^{mn}|b_n|^{m^2n}}{p}\cdot\left(\frac{L^*(f(\lambda X))}{|q|}\right)^\ell,$$

which gives the desired contradiction $|R(g^m,F_1)|<1$ if $p>|q|^{mn-\ell}|b_n|^{m^2n}L^*(f(\lambda X))^\ell$.

Case 2: $\delta\geq 2$ and $|q|>L^*(f(\lambda X))$. In this case, as $r\geq 1$, we deduce by (3.1) that

$$|R(g^m,F_1)|\leq\frac{|q|^{mn}|b_n|^{m^2n}}{p^2}\cdot\frac{L^*(f(\lambda X))}{|q|},$$

which gives the desired contradiction $|R(g^m,F_1)|<1$ if $p>|q|^{\frac{mn-1}{2}}|b_n|^{\frac{m^2n}{2}}L^*(f(\lambda X))^{\frac{1}{2}}$.

Case 3: $\delta\geq 2$ and $|q|\leq L^*(f(\lambda X))$. Here, as $r\leq mn-1$, we see by (3.1) that

$$\begin{aligned}|R(g^m,F_1)| &\leq \frac{|q|^{mn}|b_n|^{m^2n}}{p^2}\cdot\left(\frac{L^*(f(\lambda X))}{|q|}\right)^{mn-1}\\ &= \frac{1}{p^2}\cdot|q|\cdot|b_n|^{m^2n}L^*(f(\lambda X))^{mn-1},\end{aligned}$$

which gives the desired contradiction $|R(g^m,F_1)|<1$ if $p>|q|^{\frac{1}{2}}|b_n|^{\frac{m^2n}{2}}L^*(f(\lambda X))^{\frac{mn-1}{2}}$.

Summarizing, we conclude that $|R(g^m,F_1)|<1$ if

$$\begin{aligned}p &> \max\{|q|^{mn-\ell}|b_n|^{m^2n}L^*(f(\lambda X))^\ell,|q|^{\frac{mn-1}{2}}|b_n|^{\frac{m^2n}{2}}L^*(f(\lambda X))^{\frac{1}{2}},\\ &\quad |q|^{\frac{1}{2}}|b_n|^{\frac{m^2n}{2}}L^*(f(\lambda X))^{\frac{mn-1}{2}}\},\end{aligned}$$

which is precisely the hypothesis on the magnitude of p in the statement of our theorem. This completes the proof of the theorem. □

Proof of Corollary 9. Here $\ell=|q|=1$, and one may check that $\lambda\leq 1$. Therefore it suffices to ask p to satisfy

$$p>\max\{L^*(f(X)),\ L^*(f(X))^{\frac{1}{2}},\ L^*(f(X))^{\frac{m-1}{2}}\}=L^*(f(X))^{\frac{m-1}{2}},$$

as $m\geq 3$. This completes the proof. □

Proof of Corollary 10. Observe that k is coprime to m, since $k\equiv 2 \mod m$ and m is odd. Besides, for an odd $m\geq 3$ the inverse of k modulo m is $\ell=\frac{m+1}{2}\in\{1,\ldots,m-1\}$. One may check that in this case too we have $\lambda\leq 1$. Therefore it suffices to ask p to satisfy

$$p>\max\{L^*(f(X))^{\frac{m+1}{2}},\ L^*(f(X))^{\frac{1}{2}},\ L^*(f(X))^{\frac{m-1}{2}}\}=L^*(f(X))^{\frac{m+1}{2}},$$

which completes the proof. □

Proof of Theorem 5. The proof combines the ideas in the proofs of Theorem 2 and Theorem 4. Our assumption on p implies that $p>|q|^{n-\ell}|b_n|^{mn}L^*(f(\lambda X))^\ell$, so

$$\begin{aligned}p^k|q| &> |q|^{(n-\ell)k+1}|b_n|^{mnk}L^*(f(\lambda X))^{\ell k}\\ &= [\lambda^m|q|^{(n-\ell)k+1}|b_n|^{mnk}L^*(f(\lambda X))^{\ell k-1}]\cdot(|a_0|\lambda^{-m}+\cdots+|a_{m-1}|\lambda^{-1}).\end{aligned}$$

Recalling that $\lambda=(|q|^{\frac{(n-\ell)k+1}{m}}|a_0|^{\frac{\ell k-1}{m}}|b_n|^{nk})^{-1}$, we deduce that the quantity in the square brackets above is equal to

$$\left(\frac{L^*(f(\lambda X))}{|a_0|}\right)^{\ell k-1},$$

which is at least 1, as $L^*(f(\lambda X))\geq|a_0|$, and the exponent $\ell k-1$ is nonnegative.

We will consider now the situation mentioned in Remark 2. So let us assume now that

$$\lambda=(|q|^{\frac{k+2}{2m}}|a_0|^{\frac{(n-1)k-2}{2m}}|b_n|^{\frac{nk}{2}})^{-1}.$$

The hypothesis on the magnitude of p also implies that $p>|q|^{\frac{1}{2}}|b_n|^{\frac{mn}{2}}L^*(f(\lambda X))^{\frac{n-1}{2}}$, so

$$\begin{aligned}p^k|q|&>|q|^{\frac{k}{2}+1}|b_n|^{\frac{mnk}{2}}L^*(f(\lambda X))^{\frac{(n-1)k}{2}}\\&=[\lambda^m|q|^{\frac{k}{2}+1}|b_n|^{\frac{mnk}{2}}L^*(f(\lambda X))^{\frac{(n-1)k}{2}-1}]\cdot(|a_0|\lambda^{-m}+\cdots+|a_{m-1}|\lambda^{-1}).\end{aligned}$$

Here the quantity in the square brackets above is equal to

$$\left(\frac{L^*(f(\lambda X))}{|a_0|}\right)^{\frac{(n-1)k}{2}-1},$$

which is at least 1 if the exponent $\frac{(n-1)k}{2}-1$ is nonnegative. This is obviously true for $n\geq 3$, as $k\geq 1$, but also holds for $n=2$, provided $k\geq 2$ (the irreducibility of $f\circ g$ in the case that $n=1$ is obvious, as f was assumed to be irreducible).

Finally, assume that

$$\lambda=(|q|^{\frac{(n-1)k+2}{2m}}|a_0|^{\frac{k-2}{2m}}|b_n|^{\frac{nk}{2}})^{-1}.$$

Since p also satisfies the inequality $p>|q|^{\frac{n-1}{2}}|b_n|^{\frac{mn}{2}}L^*(f(\lambda X))^{\frac{1}{2}}$, we deduce that

$$\begin{aligned}p^k|q|&>|q|^{\frac{(n-1)k+2}{2}}|b_n|^{\frac{mnk}{2}}L^*(f(\lambda X))^{\frac{k}{2}}\\&=[\lambda^m|q|^{\frac{(n-1)k+2}{2}}|b_n|^{\frac{mnk}{2}}L^*(f(\lambda X))^{\frac{k}{2}-1}]\cdot(|a_0|\lambda^{-m}+\cdots+|a_{m-1}|\lambda^{-1}).\end{aligned}$$

Here the quantity in the square brackets above is equal to

$$\left(\frac{L^*(f(\lambda X))}{|a_0|}\right)^{\frac{k}{2}-1},$$

which is at least 1 if $k\geq 2$.

We have thus checked that in each of the above three cases we have

$$p^k|q|>|a_0|\lambda^{-m}+\cdots+|a_{m-1}|\lambda^{-1},$$

so here too we may still conclude that all the roots $\theta_1,\ldots,\theta_m$ of f lie in the open disk $\{|z|<\lambda\}$, and then deduce that

$$|R(g^m,F_1)|\leq\frac{|q|^{mn}|b_n|^{m^2n}}{p^\delta}\cdot\left(\frac{L^*(f(\lambda X))}{|q|}\right)^r. \tag{3.2}$$

Recall from the proof of Theorem 2 that both δ and r are positive multiples of m. In particular we may write $r = mr'$ for some integer $r' \in \{1, \ldots, n-1\}$, as $m \leq r \leq mn - m$. We again distinguish three cases:

Case 1: $\delta = m$. Observe that in this case, from the equality $\alpha mn - kmr' = -m$ we obtain $\alpha n - kr' = -1$, which implies after reduction modulo n that $kr' \equiv 1 \pmod{n}$. Thus r' must be precisely ℓ, which shows that $r = m\ell$. In this case we deduce by (3.2) that

$$\begin{aligned} |R(g^m, F_1)| &\leq \frac{|q|^{mn}|b_n|^{m^2n}}{p^m} \cdot \left(\frac{L^*(f(\lambda X))}{|q|}\right)^{m\ell} \\ &= \frac{1}{p^m} \cdot |q|^{mn-m\ell}|b_n|^{m^2n} L^*(f(\lambda X))^{m\ell}, \end{aligned}$$

which gives the desired contradiction $|R(g^m, F_1)| < 1$ if $p > |q|^{n-\ell}|b_n|^{mn} L^*(f(\lambda X))^{\ell}$.

Case 2: $\delta \geq 2m$ and $|q| > L^*(f(\lambda X))$. Since $r \geq m$, in this case we deduce by (3.2) that

$$|R(g^m, F_1)| \leq \frac{|q|^{mn}|b_n|^{m^2n}}{p^{2m}} \cdot \left(\frac{L^*(f(\lambda X))}{|q|}\right)^{m},$$

which gives the desired contradiction $|R(g^m, F_1)| < 1$ if $p > |q|^{\frac{n-1}{2}}|b_n|^{\frac{mn}{2}} L^*(f(\lambda X))^{\frac{1}{2}}$.

Case 3: $\delta \geq 2m$ and $|q| \leq L^*(f(\lambda X))$. In this third case, since $r \leq mn - m$, we deduce by (3.2) that

$$\begin{aligned} |R(g^m, F_1)| &\leq \frac{|q|^{mn}|b_n|^{m^2n}}{p^{2m}} \cdot \left(\frac{L^*(f(\lambda X))}{|q|}\right)^{mn-m} \\ &= \frac{|q|^{m} \cdot |b_n|^{m^2n} L^*(f(\lambda X))^{mn-m}}{p^{2m}}, \end{aligned}$$

which gives the desired contradiction $|R(g^m, F_1)| < 1$ if $p > |q|^{\frac{1}{2}}|b_n|^{\frac{mn}{2}} L^*(f(\lambda X))^{\frac{n-1}{2}}$.

Summarizing, we conclude that $|R(g^m, F_1)| < 1$ if

$$\begin{aligned} p \quad > \quad & \max\{|q|^{n-\ell}|b_n|^{mn} L^*(f(\lambda X))^{\ell}, |q|^{\frac{n-1}{2}}|b_n|^{\frac{mn}{2}} L^*(f(\lambda X))^{\frac{1}{2}}, \\ & |q|^{\frac{1}{2}}|b_n|^{\frac{mn}{2}} L^*(f(\lambda X))^{\frac{n-1}{2}}\}, \end{aligned}$$

which completes the proof of the theorem. □

Proof of Corollary 11. By Corollary 9, f must be irreducible over $\mathbb{Q}$. One applies then Theorem 5 with $\ell = |b_n| = |q| = 1$. □

4 The case that only the residue class of k modulo mn is known

In this section we will provide some lower bounds on p for the case that no information on the inverse ℓ of k modulo mn (or modulo n) is available, but instead, the remainder of the

Euclidean division of k by mn (or by n) is known. This will actually allow us to find upper and lower bounds for ℓ, which will still serve our purpose to properly estimate the possible degrees of the hypothetical factors of $f \circ g$. We mention here that, as the lower bounds on p depend on many parameters, in our analysis we will content ourselves with improving them without excessively complicating their expressions.

For the proof of the results in this section we need the following basic lemma, that provides some useful information on the inverse of an integer modulo n.

Lemma 1. *Let a, b and $n \geq 2$ be integers with $0 < a, b < n$ and $ab \equiv 1 \pmod{n}$. Then*

$$\frac{n-1}{n-a} \leq b \leq n - \frac{n-1}{a}. \tag{4.1}$$

Moreover, if $(a, b) \neq (1, 1)$, then we also have

$$b \geq \frac{n+1}{a}, \tag{4.2}$$

while if $(a, b) \neq (n-1, n-1)$, then we also have

$$b \leq n - \frac{n+1}{n-a}. \tag{4.3}$$

Proof. Since $ab \equiv 1 \pmod{n}$, there exists a nonnegative integer c such that $ab - 1 = cn$. As $b < n$ we deduce that $cn < an - 1$, so $c < a - \frac{1}{n}$. Thus $c \leq a - 1$, which implies that $ab - 1 \leq n(a-1)$. Therefore $ab \leq n(a-1) + 1$, which leads to the right inequality in (4.1). Interchanging now the roles of a and b in the inequality $ab \leq n(a-1) + 1$ yields $ab \leq n(b-1) + 1$, which gives the left inequality in (4.1).

If we assume now that $(a, b) \neq (1, 1)$, then our integer c must be positive, so $b = \frac{cn+1}{a} \geq \frac{n+1}{a}$. Finally, if we assume that $(a, b) \neq (n-1, n-1)$, then changing (a, b) to $(n-a, n-b)$ and using (4.2) yields $n - b \geq \frac{n+1}{n-a}$, which proves (4.3). □

Remark 3. *Notice that the integer c above is the inverse of $-n$ modulo a lying in the set $\{1, \ldots, a-1\}$. We also note that one may slightly improve the inequalities in Lemma 1 by considering the ceiling function for the lower bounds on b, and the floor function for the upper bounds on b. However, to avoid the excessive complication of the formulas in our following results, we will not make use of the floor and ceiling functions. Moreover, to keep the restrictions on k to a minimum, in our following results we will mostly use the first part of Lemma 1, namely inequalities (4.1).*

The main feature of the results in this section is that they do not require knowing the precise value of the inverse ℓ of k modulo mn (or modulo n). Instead, they rely on bounding ℓ from below and from above, thus requiring information on two suitable integers A and B such that $A \leq \ell \leq B$. In this regard, the results in our previous section correspond to the case that $A = B = \ell$.

Theorem 6. *Let $f(X) = a_0 + a_1X + \cdots + a_mX^m$ and $g(X) = b_0 + b_1X + \cdots + b_nX^n$ be non-constant polynomials with integer coefficients, with $a_0a_mb_n \neq 0$. Assume that $a_m = p^kq$ with p a prime number, q an integer, and k a positive integer coprime to mn. Let*

$\ell \in \{1, \dots, mn-1\}$ be the inverse of k modulo mn, let $A, B \in \{1, \dots, mn-1\}$ be such that $A \leq \ell \leq B$, and let

$$\lambda := \max\left\{|q|^{\frac{(mn-A)k+1}{m}}|a_0|^{\frac{Ak-1}{m}}|b_n|^{mnk}, |q|^{\frac{(mn-B)k+1}{m}}|a_0|^{\frac{Bk-1}{m}}|b_n|^{mnk}\right\}^{-1}.$$

$$\text{If } \; p > \max\Big\{|q|^{mn-A}|b_n|^{m^2n}L^*(f(\lambda X))^A, |q|^{mn-B}|b_n|^{m^2n}L^*(f(\lambda X))^B,$$
$$|q|^{\frac{mn-1}{2}}|b_n|^{\frac{m^2n}{2}}L^*(f(\lambda X))^{\frac{1}{2}}, |q|^{\frac{1}{2}}|b_n|^{\frac{m^2n}{2}}L^*(f(\lambda X))^{\frac{mn-1}{2}}\Big\},$$

then the polynomial $f \circ g$ is irreducible over $\mathbb{Q}$.

In particular, for $g(X) = X$ one obtains the following irreducibility citerion for polynomials with integer coefficients.

Corollary 12. *Let $f(X) = a_0 + a_1X + \cdots + a_mX^m$ be a non-constant polynomial with integer coefficients, with $a_0a_m \neq 0$. Assume that $a_m = p^kq$ with p a prime number, q an integer, and k a positive integer coprime to m. Let $\ell \in \{1, \dots, m-1\}$ be the inverse of k modulo m, let $A, B \in \{1, \dots, m-1\}$ be such that $A \leq \ell \leq B$, and let*

$$\lambda := \max\left\{|q|^{\frac{(m-A)k+1}{m}}|a_0|^{\frac{Ak-1}{m}}, |q|^{\frac{(m-B)k+1}{m}}|a_0|^{\frac{Bk-1}{m}}\right\}^{-1}.$$

$$\text{If } \; p > \max\big\{|q|^{m-A}L^*(f(\lambda X))^A, |q|^{m-B}L^*(f(\lambda X))^B,$$
$$|q|^{\frac{m-1}{2}}L^*(f(\lambda X))^{\frac{1}{2}}, |q|^{\frac{1}{2}}L^*(f(\lambda X))^{\frac{m-1}{2}}\Big\},$$

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

As in previous section, we can improve the conditions on p and k if we know that f is irreducible:

Theorem 7. *Let $f(X) = a_0 + a_1X + \cdots + a_mX^m$ and $g(X) = b_0 + b_1X + \cdots + b_nX^n$ be non-constant polynomials with integer coefficients, with $a_0a_mb_n \neq 0$, f irreducible over $\mathbb{Q}$. Assume that $a_m = p^kq$ with p a prime number, q an integer, and k a positive integer coprime to n. Let $\ell \in \{1, \dots, n-1\}$ be the inverse of k modulo n, let $A, B \in \{1, \dots, n-1\}$ be such that $A \leq \ell \leq B$, and let*

$$\lambda := \max\left\{|q|^{\frac{(n-A)k+1}{m}}|a_0|^{\frac{Ak-1}{m}}|b_n|^{nk}, |q|^{\frac{(n-B)k+1}{m}}|a_0|^{\frac{Bk-1}{m}}|b_n|^{nk}\right\}^{-1}.$$

$$\text{If } \; p > \max\Big\{|q|^{n-A}|b_n|^{mn}L^*(f(\lambda X))^A, |q|^{n-B}|b_n|^{mn}L^*(f(\lambda X))^B,$$
$$|q|^{\frac{n-1}{2}}|b_n|^{\frac{mn}{2}}L^*(f(\lambda X))^{\frac{1}{2}}, |q|^{\frac{1}{2}}|b_n|^{\frac{mn}{2}}L^*(f(\lambda X))^{\frac{n-1}{2}}\Big\},$$

then the polynomial $f \circ g$ is irreducible over $\mathbb{Q}$.

We mention here that one may decrease the values of λ in Theorem 6 and Theorem 7 by using the same additional terms that appear in Remark 1 and Remark 2, respectively.

To get rid of the condition that f is irreducible over $\mathbb{Q}$, and to obtain sharper irreducibility conditions than those provided by Theorem 6, one may easily combine Theorem 7 and Corollary 12. We also mention that these general results become effective whenever we can produce explicit expressions for A and B. In this respect, one may use Lemma 1, for instance, provided the remainder k' of the Euclidean division of k by mn (or by n) is known. Consider the case of Theorem 7, for instance. If $\ell \in \{1, \ldots, n-1\}$ is the inverse of k modulo n, in view of (4.1) one may take

$$A = \frac{n-1}{n-k'} \quad \text{and} \quad B = n - \frac{n-1}{k'}.$$

Moreover, if $k \not\equiv 1 \pmod{n}$, then we may also take $A = \frac{n+1}{k'}$, which is more efficient for small values of k', while if $k \not\equiv -1 \pmod{n}$, then we may also use $B = n - \frac{n+1}{n-k'}$, which is more efficient for large values of k'.

We will only present here some simple irreducibility criteria that make use of Lemma 1. We will first state two simple instances of Corollary 12.

Corollary 13. *Let $f(X) = a_0 + a_1X + \cdots + a_mX^m$ be a polynomial with integer coefficients, of degree $m \geq 3$, with $a_0 \neq 0$. Assume that $a_m = p^k$, where p is a prime number, and k is a positive integer coprime to m, $k \not\equiv 1 \pmod{m}$. Let k' be the remainder of the Euclidean division of k by m. If $p > (|a_0| + |a_1| + \cdots + |a_{m-1}|)^{m-\frac{m-1}{k'}}$, then f is irreducible over $\mathbb{Q}$.*

Corollary 14. *Let $f(X) = a_0 + a_1X + \cdots + a_mX^m$ be a polynomial with integer coefficients, of degree $m \geq 3$, with $a_0 \neq 0$. Assume that $a_m = p^k$, where p is a prime number, and k is a positive integer coprime to m, $k \not\equiv -1 \pmod{m}$. Let k' be the remainder of the Euclidean division of k by m. If $p > (|a_0| + |a_1| + \cdots + |a_{m-1}|)^{m-\frac{m+1}{m-k'}}$, then f is irreducible over $\mathbb{Q}$.*

The following three results are direct consequences of Theorem 7, and are obtained by taking $|q| = |b_n| = 1$.

Corollary 15. *Let $f(X) = a_0 + a_1X + \cdots + a_mX^m$ and $g(X) = b_0 + b_1X + \cdots + b_nX^n$ be polynomials with integer coefficients, of degrees $m \geq 1$ and $n \geq 3$, with $a_0 \neq 0$, $|b_n| = 1$, and f irreducible over $\mathbb{Q}$. Assume that $a_m = p^k$ with p a prime number and $k \equiv 1 \pmod{n}$. If $p > (|a_0| + |a_1| + \cdots + |a_{m-1}|)^{\frac{n-1}{2}}$, then $f \circ g$ is irreducible over $\mathbb{Q}$.*

For the case when $|q| = |b_n| = 1$, but $k \not\equiv 1 \pmod{n}$, we have the following result.

Corollary 16. *Let $f(X) = a_0 + a_1X + \cdots + a_mX^m$ and $g(X) = b_0 + b_1X + \cdots + b_nX^n$ be polynomials with integer coefficients, of degrees $m \geq 1$ and $n \geq 3$, with $a_0 \neq 0$, $|b_n| = 1$, and f irreducible over $\mathbb{Q}$. Assume that $a_m = p^k$ with p a prime number and k a positive integer coprime to n, $k \not\equiv 1 \pmod{n}$. Let k' be the remainder of the Euclidean division of k by n. If $p > (|a_0| + |a_1| + \cdots + |a_{m-1}|)^{n-\frac{n-1}{k'}}$, then $f \circ g$ is irreducible over $\mathbb{Q}$.*

For the case when $|q| = |b_n| = 1$, but $k \not\equiv -1 \pmod{n}$, we have the following result.

Corollary 17. *Let $f(X) = a_0 + a_1X + \cdots + a_mX^m$ and $g(X) = b_0 + b_1X + \cdots + b_nX^n$ be polynomials with integer coefficients, of degrees $m \geq 1$ and $n \geq 3$, with $a_0 \neq 0$, $|b_n| = 1$,* *and f irreducible over $\mathbb{Q}$. Assume that $a_m = p^k$ with p a prime number and k a positive integer coprime to n, $k \not\equiv -1 \pmod{n}$. Let k' be the remainder of the Euclidean division of k by n. If $p > (|a_0| + |a_1| + \cdots + |a_{m-1}|)^{n - \frac{n+1}{n-k'}}$, then $f \circ g$ is irreducible over $\mathbb{Q}$.*

To obtain results where the irreducibility of f is not apriori required, the reader may suitably combine one of Corollary 9, Corollary 13 and Corollary 14, with one of our last three results. For the sake of completeness, we will provide proofs for the results in this section too, even though they are much alike those presented in our previous sections.

Proof of Theorem 6. Here too the assumption on p implies that both q and b_n are not divisible by p. The proof follows the lines of the proof of Theorem 1.

Assume that $\lambda = (|q|^{\frac{(mn-A)k+1}{m}} |a_0|^{\frac{Ak-1}{m}} |b_n|^{mnk})^{-1}$. Our assumption on the magnitude of p implies that $p > |q|^{mn-A} |b_n|^{m^2 n} L^*(f(\lambda X))^A$, so

$$\begin{aligned} p^k |q| &> |q|^{(mn-A)k+1} |b_n|^{m^2 nk} L^*(f(\lambda X))^{Ak} \\ &= [\lambda^m |q|^{(mn-A)k+1} |b_n|^{m^2 nk} L^*(f(\lambda X))^{Ak-1}] \cdot (|a_0| \lambda^{-m} + \cdots + |a_{m-1}| \lambda^{-1}). \end{aligned}$$

In this case the quantity in the square brackets above is equal to

$$\left(\frac{L^*(f(\lambda X))}{|a_0|} \right)^{Ak-1},$$

which is at least 1, since the exponent $Ak - 1$ is nonnegative.

Assume now that $\lambda = (|q|^{\frac{(mn-B)k+1}{m}} |a_0|^{\frac{Bk-1}{m}} |b_n|^{mnk})^{-1}$. Our assumption on the magnitude of p also implies that $p > |q|^{mn-B} |b_n|^{m^2 n} L^*(f(\lambda X))^B$, so

$$\begin{aligned} p^k |q| &> |q|^{(mn-B)k+1} |b_n|^{m^2 nk} L^*(f(\lambda X))^{Bk} \\ &= [\lambda^m |q|^{(mn-B)k+1} |b_n|^{m^2 nk} L^*(f(\lambda X))^{Bk-1}] \cdot (|a_0| \lambda^{-m} + \cdots + |a_{m-1}| \lambda^{-1}). \end{aligned}$$

In this case the quantity in the square brackets above is equal to

$$\left(\frac{L^*(f(\lambda X))}{|a_0|} \right)^{Bk-1},$$

which is also at least 1, since the exponent $Bk - 1$ is nonnegative too.

We have thus checked that in each of the above two cases we have

$$p^k |q| > |a_0| \lambda^{-m} + \cdots + |a_{m-1}| \lambda^{-1}.$$

We may therefore still conclude that all the roots $\theta_1, \ldots, \theta_m$ of f lie in the open disk $\{|z| < \lambda\}$, and then deduce that

$$|R(g^m, F_1)| \leq \frac{|q|^{mn} |b_n|^{m^2 n}}{p^\delta} \cdot \left(\frac{L^*(f(\lambda X))}{|q|} \right)^r. \tag{4.4}$$

Observe now that if $\delta = 1$, then by reducing modulo mn the equality $\alpha mn - kr = -1$ we obtain $kr \equiv 1 \pmod{mn}$, so $r = \ell$, and hence

$$A \leq r \leq B. \tag{4.5}$$

We distinguish now four cases:

Case 1: $\delta = 1$ and $|q| > L^*(f(\lambda X))$. In this case we deduce by (4.4) and the left inequality in (4.5) that

$$\begin{aligned} |R(g^m, F_1)| &\leq \frac{|q|^{mn}|b_n|^{m^2n}}{p} \cdot \left(\frac{L^*(f(\lambda X))}{|q|}\right)^A \\ &= \frac{1}{p} \cdot |q|^{mn-A}|b_n|^{m^2n}L^*(f(\lambda X))^A, \end{aligned}$$

which gives the desired contradiction $|R(g^m, F_1)| < 1$ if $p > |q|^{mn-A}|b_n|^{m^2n}L^*(f(\lambda X))^A$.

Case 2: $\delta = 1$ and $|q| \leq L^*(f(\lambda X))$. In this second case, by (4.4) and the right inequality in (4.5) one obtains

$$\begin{aligned} |R(g^m, F_1)| &\leq \frac{|q|^{mn}|b_n|^{m^2n}}{p} \cdot \left(\frac{L^*(f(\lambda X))}{|q|}\right)^B \\ &= \frac{1}{p} \cdot |q|^{mn-B}|b_n|^{m^2n}L^*(f(\lambda X))^B, \end{aligned}$$

which gives the desired contradiction $|R(g^m, F_1)| < 1$ if $p > |q|^{mn-B}|b_n|^{m^2n}L^*(f(\lambda X))^B$.

Case 3: $\delta \geq 2$ and $|q| > L^*(f(\lambda X))$. As $r \geq 1$, in this case we deduce by (4.4) that

$$|R(g^m, F_1)| \leq \frac{|q|^{mn}|b_n|^{m^2n}}{p^2} \cdot \frac{L^*(f(\lambda X))}{|q|},$$

which gives the desired contradiction $|R(g^m, F_1)| < 1$ if $p > |q|^{\frac{mn-1}{2}}|b_n|^{\frac{m^2n}{2}}L^*(f(\lambda X))^{\frac{1}{2}}$.

Case 4: $\delta \geq 2$ and $|q| \leq L^*(f(\lambda X))$. Here, as $r \leq mn-1$, we deduce by (4.4) that

$$\begin{aligned} |R(g^m, F_1)| &\leq \frac{|q|^{mn}|b_n|^{m^2n}}{p^2} \cdot \left(\frac{L^*(f(\lambda X))}{|q|}\right)^{mn-1} \\ &= \frac{|q| \cdot |b_n|^{m^2n}L^*(f(\lambda X))^{mn-1}}{p^2}, \end{aligned}$$

which gives the desired contradiction $|R(g^m, F_1)| < 1$ if $p > |q|^{\frac{1}{2}}|b_n|^{\frac{m^2n}{2}}L^*(f(\lambda X))^{\frac{mn-1}{2}}$.

Summarizing, we conclude that $|R(g^m, F_1)| < 1$ if

$$\begin{aligned} p \quad > \quad & \max\{|q|^{mn-A}|b_n|^{m^2n}L^*(f(\lambda X))^A, |q|^{mn-B}|b_n|^{m^2n}L^*(f(\lambda X))^B, \\ & |q|^{\frac{mn-1}{2}}|b_n|^{\frac{m^2n}{2}}L^*(f(\lambda X))^{\frac{1}{2}}, |q|^{\frac{1}{2}}|b_n|^{\frac{m^2n}{2}}L^*(f(\lambda X))^{\frac{mn-1}{2}}\}, \end{aligned}$$

which completes the proof of the theorem. □

Proof of Theorem 7. The proof combines the ideas in the proofs of Theorem 2 and Theorem 6. Assume that $\lambda = (|q|^{\frac{(n-A)k+1}{m}}|a_0|^{\frac{Ak-1}{m}}|b_n|^{nk})^{-1}$. Our assumption on the magnitude of p implies that $p > |q|^{n-A}|b_n|^{mn}L^*(f(\lambda X))^A$, so

$$\begin{aligned} p^k|q| &> |q|^{(n-A)k+1}|b_n|^{mnk}L^*(f(\lambda X))^{Ak} \\ &= [\lambda^m|q|^{(n-A)k+1}|b_n|^{mnk}L^*(f(\lambda X))^{Ak-1}] \cdot (|a_0|\lambda^{-m} + \cdots + |a_{m-1}|\lambda^{-1}). \end{aligned}$$

In this case the quantity in the square brackets above is equal to

$$\left(\frac{L^*(f(\lambda X))}{|a_0|}\right)^{Ak-1},$$

which is at least 1, since the exponent $Ak-1$ is nonnegative.

Assume now that $\lambda = (|q|^{\frac{(n-B)k+1}{m}}|a_0|^{\frac{Bk-1}{m}}|b_n|^{nk})^{-1}$. Our assumption on the magnitude of p also implies that $p > |q|^{n-B}|b_n|^{mn}L^*(f(\lambda X))^B$, so

$$\begin{aligned}p^k|q| &> |q|^{(n-B)k+1}|b_n|^{mnk}L^*(f(\lambda X))^{Bk}\\ &= [\lambda^m|q|^{(n-B)k+1}|b_n|^{mnk}L^*(f(\lambda X))^{Bk-1}]\cdot(|a_0|\lambda^{-m}+\cdots+|a_{m-1}|\lambda^{-1}).\end{aligned}$$

In this case the quantity in the square brackets above is equal to

$$\left(\frac{L^*(f(\lambda X))}{|a_0|}\right)^{Bk-1},$$

which is also at least 1, since the exponent $Bk-1$ is nonnegative too.

We have thus checked that in each of the above two cases we have

$$p^k|q| > |a_0|\lambda^{-m}+\cdots+|a_{m-1}|\lambda^{-1},$$

so here too we may still conclude that all the roots $\theta_1,\ldots,\theta_m$ of f lie in the open disk $\{|z|<\lambda\}$, and then deduce that

$$|R(g^m,F_1)| \le \frac{|q|^{mn}|b_n|^{m^2n}}{p^\delta}\cdot\left(\frac{L^*(f(\lambda X))}{|q|}\right)^r. \tag{4.6}$$

Recall from the proof of Theorem 2 that both δ and r are positive multiples of m. In particular we may write $r = mr'$ for some integer $r' \in \{1,\ldots,n-1\}$, as $m \le r \le mn-m$. We again distinguish four cases:

Case 1: $\delta = m$ and $|q| > L^*(f(\lambda X))$. Observe that in this case, from the equality $\alpha mn - kmr' = -m$ we obtain $\alpha n - kr' = -1$, which implies after reduction modulo n that $kr' \equiv 1 \pmod n$. Thus r' must be precisely ℓ, which shows that $r = m\ell$. This implies that

$$mA \le r \le mB. \tag{4.7}$$

In this case we deduce by (4.6) and the left inequality in (4.7) that

$$\begin{aligned}|R(g^m,F_1)| &\le \frac{|q|^{mn}|b_n|^{m^2n}}{p^m}\cdot\left(\frac{L^*(f(\lambda X))}{|q|}\right)^{mA}\\ &= \frac{1}{p^m}\cdot|q|^{mn-mA}|b_n|^{m^2n}L^*(f(\lambda X))^{mA},\end{aligned}$$

which gives the desired contradiction $|R(g^m,F_1)|<1$ if $p > |q|^{n-A}|b_n|^{mn}L^*(f(\lambda X))^A$.

Case 2: $\delta = m$ and $|q| \le L^*(f(\lambda X))$. In this second case, by (4.6) and the right inequality in (4.7) one obtains

$$\begin{aligned}|R(g^m,F_1)| &\le \frac{|q|^{mn}|b_n|^{m^2n}}{p^m}\cdot\left(\frac{L^*(f(\lambda X))}{|q|}\right)^{mB}\\ &= \frac{1}{p^m}\cdot|q|^{mn-mB}|b_n|^{m^2n}L^*(f(\lambda X))^{mB},\end{aligned}$$

which gives the desired contradiction $|R(g^m, F_1)| < 1$ if $p > |q|^{n-B}|b_n|^{mn}L^*(f(\lambda X))^B$.

Case 3: $\delta \geq 2m$ and $|q| > L^*(f(\lambda X))$. Since $r \geq m$, in this case we deduce by (4.6) that

$$|R(g^m, F_1)| \leq \frac{|q|^{mn}|b_n|^{m^2 n}}{p^{2m}} \cdot \left(\frac{L^*(f(\lambda X))}{|q|}\right)^m,$$

which gives the desired contradiction $|R(g^m, F_1)| < 1$ if $p > |q|^{\frac{n-1}{2}}|b_n|^{\frac{mn}{2}}L^*(f(\lambda X))^{\frac{1}{2}}$.

Case 4: $\delta \geq 2m$ and $|q| \leq L^*(f(\lambda X))$. In this fourth case, since $r \leq mn - m$, we deduce by (4.6) that

$$\begin{aligned} |R(g^m, F_1)| &\leq \frac{|q|^{mn}|b_n|^{m^2 n}}{p^{2m}} \cdot \left(\frac{L^*(f(\lambda X))}{|q|}\right)^{mn-m} \\ &= \frac{|q|^m \cdot |b_n|^{m^2 n}L^*(f(\lambda X))^{mn-m}}{p^{2m}}, \end{aligned}$$

which gives the desired contradiction $|R(g^m, F_1)| < 1$ if $p > |q|^{\frac{1}{2}}|b_n|^{\frac{mn}{2}}L^*(f(\lambda X))^{\frac{n-1}{2}}$.

Summarizing, we conclude that $|R(g^m, F_1)| < 1$ if

$$\begin{aligned} p \quad > \quad & \max\{|q|^{n-A}|b_n|^{mn}L^*(f(\lambda X))^A, |q|^{n-B}|b_n|^{mn}L^*(f(\lambda X))^B, \\ & |q|^{\frac{n-1}{2}}|b_n|^{\frac{mn}{2}}L^*(f(\lambda X))^{\frac{1}{2}}, |q|^{\frac{1}{2}}|b_n|^{\frac{mn}{2}}L^*(f(\lambda X))^{\frac{n-1}{2}}\}, \end{aligned}$$

which completes the proof of the theorem. □

Proof of Corollary 13. If we take $|q| = 1$ in Corollary 12, we obtain

$$\lambda = \max\{|a_0|^{\frac{Ak-1}{m}}, |a_0|^{\frac{Bk-1}{m}}\}^{-1} = \frac{1}{|a_0|^{\frac{Bk-1}{m}}} \leq 1,$$

so it suffices to ask p to satisfy $p > L^*(f(X))^{\max\left\{A, B, \frac{1}{2}, \frac{m-1}{2}\right\}}$. Here $k' \geq 2$, so the bound $B = m - \frac{m-1}{k'}$ in Lemma 1 is at least $\frac{m-1}{2}$. Therefore, since $\lambda \leq 1$ it suffices to assume that $p > (|a_0| + |a_1| + \cdots + |a_{m-1}|)^{m - \frac{m-1}{k'}}$. □

Proof of Corollary 14. Here $k' \leq m - 2$, so by Lemma 1 we may take $B = m - \frac{m+1}{m-k'}$. Note that the fact that $k' \leq m-2$ forces B to be at least $\frac{m-1}{2}$. Thus, as $\lambda \leq 1$ it suffices to impose the condition $p > (|a_0| + |a_1| + \cdots + |a_{m-1}|)^{m - \frac{m+1}{m-k'}}$. □

Proof of Corollary 15. We will use Theorem 7. Note that for $|q| = |b_n| = 1$ we have

$$\lambda = \max\{|a_0|^{\frac{Ak-1}{m}}, |a_0|^{\frac{Bk-1}{m}}\}^{-1} = \frac{1}{|a_0|^{\frac{Bk-1}{m}}} \leq 1,$$

so it suffices to ask p to satisfy $p > L^*(f(X))^{\max\left\{A, B, \frac{1}{2}, \frac{n-1}{2}\right\}}$. For $k' = 1$ the bounds $A = \frac{n-1}{n-k'}$ and $B = n - \frac{n-1}{k'}$ in Lemma 1 are both equal to 1. Therefore, as $n \geq 3$, it suffices to ask p to satisfy $p > (|a_0| + |a_1| + \cdots + |a_{m-1}|)^{\frac{n-1}{2}}$. □

Proof of Corollary 16. In this case $k' \geq 2$, so the upper bound $B = n - \frac{n-1}{k'}$ is at least $\frac{n-1}{2}$. Since $\lambda \leq 1$, it suffices to assume that $p > (|a_0| + |a_1| + \cdots + |a_{m-1}|)^{n-\frac{n-1}{k'}}$. □

Proof of Corollary 17. Here $k' \leq n-2$, so the upper bound $B = n - \frac{n+1}{n-k'}$ in Lemma 1 is at least $\frac{n-1}{2}$. Since $\lambda \leq 1$, it will be sufficient to assume that p satisfies the inequality $p > (|a_0| + |a_1| + \cdots + |a_{m-1}|)^{n-\frac{n+1}{n-k'}}$. □

We will end with some examples.

5 Examples

1) Let $f(X) = 1 + a_1X + \cdots + a_{m-1}X^{m-1} + p^kqX^m$ be a polynomial with integer coefficients, of degree $m \geq 2$, with p a prime number, q an integer with $|q| \geq 2$, and k a positive integer coprime to m. If $p > 2|q|^{m-1}$ and $k > 2\log_{|q|}(|a_1| + \cdots + |a_{m-1}|)$, then f is irreducible.

To prove this, we use Corollary 4 with $a_0 = 1$ and deduce that k must satisfy the inequality

$$k > \log_{|q|^{\frac{m-1}{m}}}(|a_1| + \cdots + |a_{m-1}|) = \frac{m}{m-1} \cdot \log_{|q|}(|a_1| + \cdots + |a_{m-1}|).$$

This obviously holds, as $\frac{m}{m-1} \leq 2$, so f must be irreducible.

2) For every prime number p, the polynomial $f(X) = 2p^6 + X - X^2 + 3X^3 - X^4 + X^5$ is irreducible. It suffices to prove that the reciprocal $X^5f(\frac{1}{X}) = 2p^6X^5 + X^4 - X^3 + 3X^2 - X + 1$ is irreducible. We will use Corollary 8. In our case $q = 2$, $m = 5$, $\ell = 1$ and $|a_0| = 1$, so $\lambda = \frac{1}{2^{\frac{4\cdot 6+1}{5}}} = \frac{1}{2^5}$. Thus $L^*(f(\lambda X)) = 1 + \lambda + 3\lambda^2 + \lambda^3 + \lambda^4 < 2\lambda^2 + \frac{1}{1-\lambda} < 1.04$. The condition on p reads $p > \max\{2^4L^*(f(\lambda X)), 2^2L^*(f(\lambda X))^{\frac{1}{2}}, 2^{\frac{1}{2}}L^*(f(\lambda X))^2\}$, so to conclude that f is irreducible it suffices to ask p to satisfy $p > 2^4 \cdot 1.04 = 16.64$, that is $p \geq 17$. For the remaining values of p, we used the function `ispolirreducible` of pari/gp to check that f is irreducible.

3) Let $f(X) = a_0 + a_1X + \cdots + a_mX^m$ and $g(X) = b_0 + b_1X + \cdots + b_nX^n$ be polynomials with integer coefficients, of degrees m and n respectively, with $a_0 \neq 0$, $|b_n| = 1$ and $n \geq m \geq 3$. Assume that $|a_i| \leq 1$ for $i = 0, \ldots, m-1$ and $a_m = p^kq$ with p a prime number, q an integer with $|q| \geq 2$, and k a positive integer congruent to 1 modulo mn. If $p > 2|q|^{n-1}$, then $f \circ g$ is irreducible over $\mathbb{Q}$. To prove this, we first check the irreducibility conditions for f in Corollary 8. Since $|a_0| = \ell = 1$, we see that

$$\lambda = \frac{1}{|q|^{\frac{(m-1)k+1}{m}}} \leq \frac{1}{|q|} \leq \frac{1}{2},$$

which shows that

$$L^*(f(\lambda X)) \leq 1 + \frac{1}{2} + \cdots + \frac{1}{2^{m-1}} < 2.$$

The condition on the magnitude of p reduces to

$$\begin{aligned} p &> \max\{|q|^{m-1}L^*(f(\lambda X)), |q|^{\frac{m-1}{2}}L^*(f(\lambda X))^{\frac{1}{2}}, |q|^{\frac{1}{2}}L^*(f(\lambda X))^{\frac{m-1}{2}}\} \\ &= |q|^{m-1}L^*(f(\lambda X)), \end{aligned}$$

as $|q| \geq 2 > L^*(f(\lambda X))$. To conclude that f is irreducible over $\mathbb{Q}$ it is therefore sufficient to ask p to satisfy the inequality $p > 2|q|^{m-1}$. We check now the conditions in Theorem 5. Since $|b_n| = |a_0| = \ell = 1$, we see that here

$$\lambda = \frac{1}{|q|^{\frac{(n-1)k+1}{m}}} \leq \frac{1}{|q|^{\frac{n}{m}}} \leq \frac{1}{|q|} \leq \frac{1}{2},$$

as $n \geq m$, so in this case too we have $L^*(f(\lambda X)) < 2$. The condition on p reduces to

$$\begin{aligned} p &> \max\{|q|^{n-1}L^*(f(\lambda X)), |q|^{\frac{n-1}{2}}L^*(f(\lambda X))^{\frac{1}{2}}, |q|^{\frac{1}{2}}L^*(f(\lambda X))^{\frac{n-1}{2}}\} \\ &= |q|^{n-1}L^*(f(\lambda X)), \end{aligned}$$

again since $|q| \geq 2 > L^*(f(\lambda X))$. To conclude that $f \circ g$ is irreducible over $\mathbb{Q}$ it is therefore sufficient to ask $p > 2|q|^{n-1}$, which also implies our previous condition $p > 2|q|^{m-1}$, as $n \geq m$.

4) For every monic polynomial $g(X) \in \mathbb{Z}[X]$ of degree $n \geq 3$, every positive integer a, and every prime number $p > 3^{n-1}$, the polynomial $1 + 2g(X) + p^{an-1}g(X)^2$ is irreducible over $\mathbb{Q}$. To check this, we write this polynomial as $f \circ g(X)$ with $f(X) = 1 + 2X + p^{an-1}X^2$, and we observe that f is irreducible over $\mathbb{Q}$, having negative discriminant. Here $k = an - 1$, so $k' = n - 1$. By Corollary 16 we then conclude that $f \circ g$ is irreducible over $\mathbb{Q}$ if $p > (1+2)^{n-\frac{n-1}{n-1}} = 3^{n-1}$.

Acknowledgement. This paper was partially supported by a GDRI ECO-Math project.

References

[1] M. Ayad, Irreducibility of f(u(x), v(y)), *J. Algebra*, **279**, 302–307 (2004).

[2] L. Bary-Soroker, Irreducible values of polynomials, *Adv. Math.*, **229**, 854–874 (2012).

[3] L. Bary-Soroker, A. Entin, Explicit Hilbert's irreducibility theorem in function fields, Abelian varieties and number theory, *Contemp. Math.*, **767**, Providence, RI, 125–134 (2021).

[4] A. Bodin, P. Dèbes, S. Najib, The Schinzel hypothesis for polynomials, *Trans. Amer. Math. Soc.*, **373**, 8339–8364 (2020).

[5] A. Bodin, P. Dèbes, S. Najib, Families of polynomials and their specializations, *J. Number Theory*, **170**, 390–408 (2017).

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

[7] A. I. Bonciocat, N. C. Bonciocat, A Capelli type theorem for multiplicative convolutions of polynomials, *Math. Nachr.*, **281**, 1240–1253 (2008).

[8] A. I. Bonciocat, N. C. Bonciocat, M. Cipu, Irreducibility criteria for compositions and multiplicative convolutions of polynomials with integer coefficients, *An. Şt. Univ. Ovidius Constanţa*, **22**, 73–84 (2014).

[9] A. I. Bonciocat, N. C. Bonciocat, A. Zaharescu, On the number of factors of convolutions of polynomials with integer coefficients, *Rocky Mountain J. Math.*, **38**, 417–431 (2008).

[10] A. I. Bonciocat, A. Zaharescu, Irreducibility results for compositions of polynomials with integer coefficients, *Monatsh. Math.*, **149**, 31–41 (2006).

[11] A. I. Bonciocat, A. Zaharescu, Irreducibility results for compositions of polynomials in several variables, *Proc. Indian Acad. Sci. (Math. Sci.)*, **115**, 117–126 (2005).

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

[13] N. C. Bonciocat, An irreducibility criterion for the sum of two relatively prime polynomials, *Funct. Approx. Comment. Math.*, **54**, 163–171 (2016).

[14] N. C. Bonciocat, Irreducibility criteria for compositions of multivariate polynomials, *Acta Math. Hungar.*, **156**, 172–181 (2018).

[15] N. C. Bonciocat, Y. Bugeaud, M. Cipu, M. Mignotte, Some Pólya type irreducibility criteria for multivariate polynomials, *Comm. Algebra*, **40**, 3733–3744 (2012).

[16] N. C. Bonciocat, Y. Bugeaud, M. Cipu, M. Mignotte, Irreducibility criteria for compositions of polynomials with integer coefficients, *Monath. Math.*, **182**, 499–512 (2017).

[17] A. Brauer, R. Brauer, Über Irreduzibilitätskriterien von I. Schur und G. Pólya, *Math. Z.*, **40**, 242–265 (1935).

[18] A. Brauer, R. Brauer, H. Hopf, Über die Irreduzibilität einiger spezieller Klassen von Polynomen, *Jahresber. Deutsch Math.-Verein.*, **35**, 99–112 (1926).

[19] A. Capelli, Sulla riduttibilità delle equazioni algebriche, Nota prima, *Rend. Accad. Sc. Fis. Mat. Soc. Napoli*, **3**, 243–252 (1897).

[20] A. Castillo, R. Dietmann, On Hilbert's irreducibility theorem, *Acta Arith.*, **180**, 1–14 (2017).

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

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

[23] M. Cavachi, M. Vâjâitu, A. Zaharescu, An irreducibility criterion for polynomials in several variables, *Acta Math. Univ. Ostrav.*, **12**, 13–18 (2004).

[24] P. Corvaja, Rational fixed points for linear group actions, *Ann. Sc. Norm. Super. Pisa Cl. Sci.*, **6**, 561–597 (2007).

[25] P. Dèbes, G-fonctions et théorème d'irréductibilité de Hilbert, *Acta Arith.*, **47**, 371–402 (1986).

[26] P. Dèbes, Parties hilbertiennes et progressions géométriques, *C. R. Acad. Sci. Paris Sér. I Math.*, **302**, 87–90 (1986).

[27] P. Dèbes, On the irreducibility of the polynomials $p(t^m, y)$, *J. Number Theory*, **42**, 141–157 (1992).

[28] P. Dèbes, Hilbert subsets and s-integral points, *Manuscripta Mathematica*, **89**, 107–137 (1996).

[29] P. Dèbes, Reduction and specialization of polynomials, *Acta Arith.*, **172**, 175–197 (2016).

[30] P. Dèbes, Y. Walkowiak, Bounds for Hilbert's irreducibility theorem, *Pure Appl. Math. Q.*, **4**, 1059–1083, Special issue: In honor of Jean-Pierre Serre, Part 1 (2008).

[31] H. L. Dorwart, O. Ore, Criteria for the irreducibility of polynomials, *Ann. of Math.*, **34**, 81–94 (1933).

[32] G. Dumas, Sur quelques cas d'irreductibilité des polynômes á coefficients rationnels, *Journal de Math. Pure et Appl.*, **2**, 191–258 (1906).

[33] R. Dvornicich, U. Zannier, Cyclotomic Diophantine problems (Hilbert irreducibility and invariant sets for polynomial maps), *Duke Math. J.*, **139**, 527–554 (2007).

[34] W. Flügel, Lösung der Aufgabe 226, *Archiv der Math. und Phys.*, **15**, 271–272 (1909).

[35] M. Fried, On Hilbert's irreducibility theorem, *J. Number Theory*, **6**, 211–231 (1974).

[36] N. H. Guersenzvaig, Elementary criteria for irreducibility of $f(X^r)$, *Israel J. Math.*, **169**, 109–123 (2009).

[37] K. Győry, Sur l'irreducibilité d'une classe des polynômes. I, *Publ. Math. Debrecen*, **18**, 289–307 (1972).

[38] K. Győry, Sur l'irreducibilité d'une classe des polynômes. II, *Publ. Math. Debrecen*, **19**, 293–326 (1973).

[39] K. Győry, On the irreducibility of a class of polynomials. III, *J. Number Theory*, **15**, 164–181 (1982).

[40] K. Győry, On the irreducibility of a class of polynomials. IV, *Acta Arith.*, **62**, 399–405 (1992).

[41] K. Győry, On the irreducibility of neighbouring polynomials, *Acta Arith.*, **67**, 283–294 (1994).

[42] K. Győry, L. Hajdu, R. Tijdeman, Irreducibility criteria of Schur-type and Pólya-type, *Monatsh. Math.*, **163**, 415–443 (2011).

[43] H. Ille, Einige Bemerkungen zu einem von G. Pólya herrührenden Irreduzibilitätskriterium, *Jahresber. Deutsch. Math.-Verein.*, **35**, 204–208 (1926).

[44] K. Langmann, Der Hilbertsche Irreduzibilitätssatz und Primzahlfragen, *J. Reine Angew. Math.*, **413**, 213–219 (1991).

[45] Y. Morita, A note on the Hilbert irreducibility theorem, *Proc. Japan Acad. Ser. A*, **66**, 101–104 (1990).

[46] P. Müller, Finiteness results for Hilbert's irreducibility theorem, *Ann. Inst. Fourier (Grenoble)*, **52**, 983–1015 (2002).

[47] L. Panaitopol, D. Ştefănescu, A resultant condition for the irreducibility of the polynomials, *J. Number Theory*, **25**, 107–111 (1987).

[48] L. Panaitopol, D. Ştefănescu, Polynomial Factorizations, *Bull. Math. Soc. Sci. Math. Roumanie*, **49 (97)**, 69–74 (2006).

[49] G. Pólya, G. Szegö, *Aufgaben und Lehrsätze aus der Analysis, Band II*, 3rd ed. Berlin, Springer (1964).

[50] L. Rédei, *Algebra, vol. 1*, translated from Hungarian, Pergamon Press, Oxford (1967).

[51] A. Schinzel, *Selected Topics on Polynomials*, University of Michigan Press, Ann Arbor (1982).

[52] A. Schinzel, *Polynomials with Special Regard to Reducibility*, Encyclopedia Math. Appl. 77, Cambridge Univ. Press (2000).

[53] I. Seres, Lösung und Verallgemeinerung eines Schurschen Irreduzibilitätsproblems für Polynome, *Acta Math. Acad. Sci. Hung.*, **7**, 151–157 (1956).

[54] I. Seres, Über die Irreduzibilität gewisser Polynome, *Acta Arith.*, **8**, 321–341 (1963).

[55] I. Seres, Irreducibility of Polynomials, *J. Algebra*, **2**, 283–286 (1965).

[56] V. G. Sprindžuk, Arithmetic specializations in polynomials, *J. Reine Angew. Math.*, **340**, 26–52 (1983).

[57] D. Ştefănescu, On the factorization of polynomials over discrete valuation domains, *An. Şt. Univ. Ovidius, Constanţa*, **22**, 273–280 (2014).

[58] U. Wegner, Über die Irreduzibilität einer Klasse von ganzen rationalen Funktionen, *Jahresber. Deutsch. Math.-Verein.*, **40**, 239–241 (1931).

[59] U. Zannier, Hilbert irreducibility above algebraic groups, *Duke Math. J.*, **153**, 397–425 (2010).

Received: 26.02.2022
Accepted: 07.04.2022

[1] University of California, Los Angeles, CA 90095, USA
E-mail: `cmbonciocat@gmail.com`

[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`