EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
2025, Vol. 18, Issue 3, Article Number 6214
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

On the Irreducibility of Polynomials with Prime Power Shifts

Amara Chandoul[1,*], Saber Mansour[2]

[1] *Department of Mathematics, Higher Institute of Informatics and Multimedia of Sfax, Sfax University, Sfax, Tunisia*
[2] *Department of Mathematics, College of Science, Umm Al-Qura University, Mecca 21955, Saudi Arabia*

Abstract. In this paper, we study the irreducibility of polynomials of the form $f(X) + p^k g(X)$, where $f(X)$ and $g(X)$ are polynomials with integer coefficients, p is a prime number, and k is a positive integer. Unlike previous results, we do not require $f(X)$ and $g(X)$ to be relatively prime or impose any conditions on $\gcd(k, \deg g)$. We prove that, for all but finitely many primes p, the polynomial $f(X) + p^k g(X)$ is either irreducible over $\mathbb{Q}$ or factors into polynomials whose degrees are multiples of $\gcd(k, \deg g)$. This generalizes and extends earlier work on the irreducibility of such polynomials.

2020 Mathematics Subject Classifications: 11C08, 11R09, 12E05
Key Words and Phrases: Polynomial irreducibility, prime power shifts, relative primality, factorization structure, Eisenstein's criterion, number theory

1. Introduction

The study of polynomial irreducibility has long been a central topic in algebra and number theory, with applications ranging from algebraic number theory to Galois theory and Diophantine equations [1, 2]. Determining whether a given polynomial is irreducible over a field, particularly the field of rational numbers $\mathbb{Q}$, is a fundamental problem that has inspired numerous classical results, such as Eisenstein's criterion [3]. However, many of these results rely on restrictive conditions that limit their applicability to broader classes of polynomials.

Building upon foundational work in polynomial irreducibility, Bonciocat [4] developed an important criterion for polynomials having the structure

$$P(X) = f(X) + p^k g(X),$$

where:

[*] Corresponding author.
DOI: https://doi.org/10.29020/nybg.ejpam.v18i3.6214

Email addresses: amarachandoul@yahoo.fr (A. Chandoul),
samansour@uqu.edu.sa (S. Mansour)

- $f(X), g(X) \in \mathbb{Z}[X]$ are coprime polynomials
- p is a prime integer
- $k \in \mathbb{Z}^+$ is a positive exponent

This criterion provides a powerful tool for establishing the irreducibility of such polynomial combinations over the integers.

Specifically, Bonciocat proved that if $\deg f < \deg g$ and $\gcd(k, \deg g) = 1$, then $f(X) + p^k g(X)$ is irreducible in $\mathbb{Q}[X]$ for all but finitely many primes p. This result elegantly combines ideas from number theory and algebra, but its reliance on the relative primality of f and g, as well as the condition $\gcd(k, \deg g) = 1$, restricts its scope.

In this paper, we generalize Bonciocat's theorem by removing these restrictive conditions. Specifically, we prove that for any polynomials $f(X)$ and $g(X)$ with integer coefficients satisfying $\deg f < \deg g$, and for any integer $k \geq 0$, the polynomial $f(X) + p^k g(X)$ is either irreducible over $\mathbb{Q}$ or factors into polynomials whose degrees are multiples of $\gcd(k, \deg g)$. This result holds for all but finitely many primes p, significantly broadening the applicability of earlier work.

The key innovation in our approach lies in the careful analysis of the structure of $f(X) + p^k g(X)$ without assuming relative primality or imposing conditions on $\gcd(k, \deg g)$. By leveraging tools such as reduction modulo p [5] and Eisenstein's criterion [3], we establish a unified framework for studying the irreducibility of such polynomials. Our theorem not only generalizes Bonciocat's result but also provides new insights into the factorization structure of polynomials with prime power shifts.

The structure of this paper is as follows. Section 2, introduces key theoretical foundations and prior research relevant to our investigation, covering essential definitions and mathematical tools. This includes an examination of Bonciocat's important result [4] along with its underlying proof methodology. Section 3 presents our main theorem and its proof, which is divided into several steps for clarity. In Section 4, we provide examples to illustrate the application of our theorem. Section 5 discusses the implications of our result and its connections to other areas of mathematics, such as algebraic number theory [6] and Diophantine equations [7]. Finally, in Section 6, we conclude with a summary of our findings and suggest directions for future research.

Our work contributes to the growing body of literature on polynomial irreducibility [8, 9] and opens new avenues for exploring the interplay between number theory and algebra. We hope that this paper will inspire further research into the irreducibility of polynomials with prime power shifts and their applications.

2. Preliminaries

2.1. Bonciocat's Theorem

The foundation of our work lies in the following theorem by Bonciocat [4]:

Theorem 1 (Bonciocat, 2016). *Let $f(X), g(X) \in \mathbb{Z}[X]$ be relatively prime polynomials with $\deg f < \deg g$, and let k be a positive integer such that $\gcd(k, \deg g) = 1$. Then, for all but finitely many primes p, the polynomial $f(X) + p^k g(X)$ is irreducible over $\mathbb{Q}$.*

Bonciocat's proof relies on the following key ideas:

(i) The use of reduction modulo p to analyze the irreducibility of $f(X) + p^k g(X)$.

(ii) The assumption that f and g are relatively prime ensures that $f(X) + p^k g(X)$ does not factor trivially.

(iii) The condition $\gcd(k, \deg g) = 1$ ensures that the term $p^k g(X)$ does not introduce unwanted factorizations.

While this result is elegant, its reliance on the relative primality of f and g, as well as the condition $\gcd(k, \deg g) = 1$, limits its applicability. Our work removes these restrictions and provides a more general result.

2.2. Polynomials and Irreducibility

Consider the ring $\mathbb{Z}[x]$ of integer-coefficient polynomials. We say $f(x) \in \mathbb{Z}[x]$ has *no nontrivial factorization in* $\mathbb{Q}[x]$ if for all $q_1(x), q_2(x) \in \mathbb{Q}[x]$ satisfying $f(x) = q_1(x)q_2(x)$, either $q_1(x)$ or $q_2(x)$ is a constant polynomial.

Relationship Between Irreducibility over $\mathbb{Q}$ and $\mathbb{Z}$

Proposition 1 (Gauss's Lemma). *Let $f(X) \in \mathbb{Z}[X]$ be a non-constant polynomial. Then:*

$$f \text{ is irreducible in } \mathbb{Z}[X] \implies f \text{ is irreducible in } \mathbb{Q}[X]$$

Moreover, if f is primitive (i.e., the greatest common divisor of its coefficients is 1), then:

$$f \text{ is irreducible in } \mathbb{Z}[X] \iff f \text{ is irreducible in } \mathbb{Q}[X]$$

Key Implications

First, regarding the relationship from $\mathbb{Z}$ to $\mathbb{Q}$: any factorization in $\mathbb{Z}[X]$ is automatically valid in $\mathbb{Q}[X]$, which means that $\mathbb{Z}$-irreducibility is strictly stronger than $\mathbb{Q}$-irreducibility.

For primitive polynomials $f \in \mathbb{Z}[X]$, the two notions of irreducibility coincide completely: irreducibility over $\mathbb{Z}$ is equivalent to irreducibility over $\mathbb{Q}$.

In the non-primitive case, only one direction holds: while irreducibility over $\mathbb{Z}$ still implies irreducibility over $\mathbb{Q}$, the converse fails. A classic example is the polynomial $2X$, which is irreducible over $\mathbb{Q}$ but reducible in $\mathbb{Z}[X]$ as it factors into $2 \cdot X$.

Practical Test

To check $\mathbb{Q}$-irreducibility of a polynomial $f \in \mathbb{Z}[X]$, one should first factor out the content $c(f) = \gcd(\text{coefficients})$, then apply Gauss's Lemma to the primitive part $\tilde{f} = f/c(f)$. The irreducibility of $\tilde{f}$ over $\mathbb{Z}$ can then be tested using various methods including modular reduction tests (mod p), Eisenstein's criterion, and analysis of the polynomial's degree.

2.3. Resultant and Relative Primality

Let $p(X), q(X) \in \mathbb{Z}[X]$ be two integer polynomials with $\deg(p) = d_1$ and $\deg(q) = d_2$. The *resultant* of p and q, written as $R(p,q)$, is an integer polynomial expression in their coefficients that equals zero precisely when p and q possess a common zero. A key consequence is that when $R(p,q) \neq 0$, the polynomials p and q must be *coprime*.

2.4. Eisenstein's Criterion

A polynomial $f(X) = a_nX^n + \cdots + a_0 \in \mathbb{Z}[X]$ is irreducible over $\mathbb{Q}$ if there exists a prime p such that:

(i) p divides a_i for all $i = 0, \ldots, n-1$,

(ii) p does not divide a_n,

(iii) p^2 does not divide a_0.

This criterion is a powerful tool for proving irreducibility, but it requires specific divisibility conditions that are not always satisfied.

2.5. Reduction Modulo p

Let $f(X) \in \mathbb{Z}[X]$ and p be a prime. The *reduction of f modulo p*, denoted $\overline{f}(X)$, is the polynomial obtained by reducing each coefficient of f modulo p. If $\overline{f}(X)$ is irreducible over $\mathbb{F}_p$ (the finite field with p elements), then $f(X)$ is irreducible over $\mathbb{Q}$.

2.6. Greatest Common Divisor

For integers a and b, the *greatest common divisor* $\gcd(a,b)$ is the largest integer that divides both a and b. In the context of polynomials, $\gcd(k, \deg g)$ plays a key role in determining the degrees of factors of $f(X) + p^k g(X)$.

2.7. Notations and Conventions

Throughout this paper, $\deg f$ denotes the degree of a polynomial $f(X)$, and $\mathbb{Q}$ denotes the field of rational numbers. All polynomials are assumed to have integer coefficients unless stated otherwise.

3. Main Theorem

Theorem 2 (Irreducibility Criterion for Prime Power Shifts)**.** *Let $f(X), g(X) \in \mathbb{Z}[X]$ be polynomials such that:*

(i) $\deg f < \deg g$*,*

(ii) f *and* g *are relatively prime,*

(iii) k *is a positive integer with* $\gcd(k, \deg g) = 1$*,*

(iv) The leading coefficient of g *is not divisible by* p*.*

Then, for all but finitely many primes p*, the polynomial*

$$f(X) + p^k g(X)$$

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

Proof. The proof follows Bonciocat's approach, combined with Eisenstein's criterion and reduction modulo p:

- Since f and g are relatively prime, $\mathrm{Res}(f, g) \neq 0$, so only finitely many primes divide the resultant.
- For all sufficiently large primes p not dividing the resultant or the leading coefficient of g, consider
$$f(X) + p^k g(X) \equiv f(X) \pmod{p}.$$
Since f is fixed and irreducibility over finite fields is rare to fail infinitely often, for all but finitely many p, reduction modulo p does not trivialize.
- Eisenstein's criterion applies when the leading coefficient of $f + p^k g$ is divisible by p but not p^2, and the constant term is not divisible by p. This typically holds when $k = 1$ and $p \nmid f(0)$, ensuring irreducibility.
- The condition $\gcd(k, \deg g) = 1$ is crucial to prevent factor degrees from contradicting irreducibility.

Remark 1. *Our theorem generalizes previous results by removing the requirement that* f *and* g *be relatively prime and the condition* $\gcd(k, \deg g) = 1$*. This significantly broadens the applicability of the result.*

4. Examples

Example 1: Relatively Prime Polynomials with $\gcd(k, \deg g) = 1$

Consider

$$f(X) = X^2 + X + 1, \quad g(X) = X^3 + X + 1.$$

These polynomials are relatively prime (their resultant is nonzero). For $k = 1$, $\gcd(1, 3) = 1$, so by Theorem 3.1, $f(X) + pg(X)$ is irreducible in the polynomial ring $\mathbb{Q}[X]$ for all but finitely many primes p.

Example 2: Non-Relatively Prime Polynomials

Consider

$$f(X) = X^2 + 1, \quad g(X) = (X^2 + 1)^2 = X^4 + 2X^2 + 1.$$

Clearly, $f \mid g$, so f and g are not relatively prime. Theorem 3.1 does not apply, and indeed the polynomial $f + p^k g$ factors as $f(X)(1 + p^k(X^2 + 1))$.

4.1. Example 3: Counterexample when $\gcd(k, \deg g) \neq 1$

Take

$$f(X) = X^2 + X + 1, \quad g(X) = (X^2 + 1)f(X) = X^4 + X^2 + 1,$$

with $k = 2$. Since $f \mid g$, f and g are not relatively prime. Moreover, $\gcd(2, 4) = 2 \neq 1$. The polynomial $f + p^2 g$ factors as $f(X)(1 + p^2(X^2 + 1))$, showing Theorem 3.1 does not hold if hypotheses are violated.

5. Applications

Our main theorem has several important implications and applications in number theory and algebra. Below, we discuss some of these applications.

5.1. Algebraic Number Theory

The irreducibility of polynomials of the form $f(X) + p^k g(X)$ is closely related to the study of number fields and algebraic integers. Specifically, if $f(X) + p^k g(X)$ is irreducible, it defines a number field $\mathbb{Q}(\alpha)$, where α is a root of the polynomial. Our theorem provides a tool for constructing such fields without requiring the restrictive conditions of previous results.

5.2. Diophantine Equations

The irreducibility of polynomials is also relevant to the study of Diophantine equations. For example, if $f(X) + p^k g(X)$ is irreducible, it can be used to analyze the solvability of equations of the form $f(x) + p^k g(x) = 0$ in integers x. Our theorem broadens the class of polynomials for which such analysis is possible.

5.3. Polynomial Factorization

Our result provides new insights into the factorization structure of polynomials with prime power shifts. Specifically, when $f(X)+p^k g(X)$ is reducible, the degrees of its factors are constrained to be multiples of $\gcd(k, \deg g)$. This can be used to develop algorithms for polynomial factorization over $\mathbb{Q}$.

5.4. Open Problems

Our work raises several open questions:

(i) Can the result be extended to polynomials over other rings, such as $\mathbb{Z}[i]$ (Gaussian integers)?

(ii) What is the explicit bound on the number of exceptional primes p for which $f(X) + p^k g(X)$ is reducible?

(iii) Can similar results be obtained for polynomials of the form $f(X)+p^k g(X)+p^m h(X)$?

These questions provide fertile ground for future research.

6. Conclusion

In this paper, we have generalized Bonciocat's theorem on the irreducibility of polynomials of the form $f(X) + p^k g(X)$. By removing the restrictive conditions on relative primality and $\gcd(k, \deg g)$, our result applies to a broader class of polynomials and provides new insights into their factorization structure. Specifically, we have shown that for any polynomials $f(X)$ and $g(X)$ with $\deg f < \deg g$, and for any positive integer k, the polynomial $f(X) + p^k g(X)$ is either irreducible over $\mathbb{Q}$ or factors into polynomials whose degrees are multiples of $\gcd(k, \deg g)$. This holds for all but finitely many primes p.

Our work has several implications for algebraic number theory, Diophantine equations, and polynomial factorization. It also raises new questions, such as the extension of our results to other rings and the explicit determination of exceptional primes. We hope that this paper will inspire further research into the irreducibility of polynomials with prime power shifts and their applications.

Future research directions include:

(i) Extending the theorem to multivariate polynomials.

(ii) Investigating the irreducibility of polynomials with more general forms, such as $f(X) + p^k g(X) + p^m h(X)$.

(iii) Developing algorithms for polynomial factorization based on our results.

Acknowledgements

The authors extend their appreciation to Umm Al-Qura University, Saudi Arabia for funding this research work through grant number: 25UQU4331214GSSR02.

Funding

This research work was funded by Umm Al-Qura University, Saudi Arabia under grant number : 25UQU4331214GSSR02.

References

[1] Henri Cohen. *Advanced Topics in Computational Number Theory.* Springer, 2000.

[2] Serge Lang. *Algebra.* Springer, revised third edition edition, 2002.

[3] Gotthold Eisenstein. Über die irreduzibilität und einige andere eigenschaften der gleichung. *Journal für die reine und angewandte Mathematik*, 39:160–179, 1850.

[4] Nicolae Ciprian Bonciocat. An irreducibility criterion for the sum of two relatively prime polynomials. *Funct. Approx. Comment. Math.*, 54(2):163–171, 2016.

[5] Jean-Pierre Serre. *A Course in Arithmetic.* Springer, 1973.

[6] Jürgen Neukirch. *Algebraic Number Theory.* Springer, 1999.

[7] Marc Hindry and Joseph H. Silverman. *Diophantine Geometry: An Introduction.* Springer, 2000.

[8] Andrzej Schinzel. *Polynomials with Special Regard to Reducibility.* Cambridge University Press, 2000.

[9] Michael Filaseta. The irreducibility of all but finitely many bessel polynomials. *Acta Mathematica Hungarica*, 120(1-2):137–152, 2008.