EUROPEAN JOURNAL OF PURE AND APPLIED MATHEMATICS
2026, Vol. 19, Issue 1, Article Number 7285
ISSN 1307-5543 – ejpam.com
Published by New York Business Global

A Fundamental Factorization Lemma Revisited

Rishu Garg[1,*] Jitender Singh[1]

[1] *Department of Mathematics, Guru Nanak Dev University, Amritsar 143005, India*

Abstract. Lemma 3 in the paper [1] [*Communications in Algebra*, **49**(6), 2722–2727, 2021] is revisited. In this paper, we provide an improvised rudimentary proof of the same.

2020 Mathematics Subject Classifications: 12E05, 11C08, 11R09

Key Words and Phrases: Irreducibility of polynomials, integer coefficients, irreducibility criterion

1. Introduction

Irreducibility of polynomials having integer coefficients has been an exciting theme of mathematical research, since the classical irreducibility criteria due to Schönemann [2], Eisenstein [3], and Dumas [4], and such research studies have close connection with prime numbers (see [5, 6]). Over the years, a number of irreducibility criteria for testing irreducibility of polynomials over integers have been obtained in the literature and the reader is referred to see the comprehensive review in [7]. It is well acknowledged that the classical irreducibility criteria due to Schönemann [2] and Eisenstein [3] are immediate consequences of a prolific general factorization result due to Dumas [4] predicated on the exciting Newton polygon approach that gives an instantaneous proof of Lemma 3 of [1] (mentioned below) which further paves the way for irreducibility criteria, viz., Theorems 1 & 2 of [1], Conjecture 1.5 in [8], a generalization of Girstmair's irreducibility criterion [9] in [10, Theorem 3.1] and a factorization result in [11, Theorem 1] as a generalization of Eisenstein's irreducibility criterion. The Lemma 3 of [1] is stated as follows:

Lemma 1 (Singh and Kumar [1])**.** *Let* $f = a_0+a_1x+\cdots+a_nx^n$, $f_1 = b_0+b_1x+\cdots+b_mx^m$, *and* $f_2 = c_0 + c_1x + \cdots + c_{n-m}x^{n-m}$ *be nonconstant polynomials in* $\mathbb{Z}[x]$ *such that* $f(x) = f_1(x)f_2(x)$. *Suppose there exists a prime number* p *and positive integers* $k \geq 2$ *and* $j \leq n$ *such that* $p^k \mid \gcd(a_0, a_1, \ldots, a_{j-1})$, $p^{k+1} \nmid a_0$, *and* $\gcd(k, j) = 1$. *If* $p \mid b_0$ *and* $p \mid c_0$, *then* $p \mid a_j$.

*Corresponding author.
DOI: https://doi.org/10.29020/nybg.ejpam.v19i1.7285
Email addresses: rishugarg128@gmail.com (R. Garg), jitender.math@gndu.ac.in (J. Singh)

For the interested reader, we mention here that Lemma 1 has been generalized in [12, Lemma 8] thereby yielding a generalization of the classical Dumas irreducibility criterion [4] as well as the irreducibility result of Weintraub [13], and several generalizations and extensions of Girstmair's irreducibility criterion in the papers [14] and [15].

For a prime number p, let v_p denote the p-adic valuation of the field of rational numbers. Thus, for any positive integer a, $v_p(a)$ is the nonnegative integer for which $p^{v_p(a)}$ divides a but $p^{1+v_p(a)}$ does not divide a, where $v_p(0) = \infty$. The p-adic valuation on $\mathbb{Q}$ is a particular example of discrete valuation with the value group $\mathbb{Z}$ and such valuations are used in the theory of Newton polygons, which in turn connect the factorization properties of underlying polynomials via the Newton polygons of the factors (see for instance, [4, 16]). The Newton polygon $NP(f)$ of a polynomial $f = a_0 + a_1x + \cdots + a_nx^n \in \mathbb{Z}[x]$ with respect to a prime p is defined as the polygonal path formed by taking the lower convex hull of the set of points $\{(i, v_p(a_i)) \mid i = 0, 1, \ldots, n\}$ in the cartesian plane $\mathbb{R}^2$. Each segment of the polygonal path so obtained is called an edge of $NP(f)$ and the point at which two edges of distinct slopes meet is called a vertex of $NP(f)$. Using these notations and definitions, we provide an alternative proof of Lemma 1 using the following fundamental result of Dumas [4].

Theorem A (Dumas)**.** *Let $f = f_1f_2$ where f, f_1, and f_2 are nonconstant polynomials in $\mathbb{Z}[x]$, with $f_1(0)f_2(0) \neq 0$ and let p be a prime number. Then the edges of the Newton polygon of f with respect to p are formed by translating and combining the edges of the Newton polygons of f_1 and f_2 with respect to p, with the slopes of the edges increasing.*

An alternative proof of Lemma 1] Let $v = v_p$. Suppose on the contrary that $v(a_j) = 0$. In $NP(f)$, the Newton polygon of f with respect to the prime p, there is an edge joining the vertices $A(0, v(a_0)) = (0, k)$ and $B(j, v(a_j)) = (j, 0)$ of slope $-k/j < 0$. Since $\gcd(k, j) = 1$, there is no lattice point, that is, a point having integer coordinates on AB other than the points A and B. Further, AB is the only edge with negative slope on $NP(f)$. Since $v(a_j) = 0$, there exist smallest indices $r \leq m$ and $s \leq n - m$ for which $v(b_r) = 0 = v(c_s)$. Since $v(b_0) > 0$ and $v(c_0) > 0$, there is an edge on the Newton polygon $NP(f_1)$ with respect to p, joining the vertices $(0, v(b_0))$ and $(r, 0)$ of slope $-v(b_0)/r < 0$. Similarly, there is an edge on the Newton polygon $NP(f_2)$ with respect to p, joining the vertices $(0, v(c_0))$ and $(s, 0)$ of slope $-v(c_0)/s < 0$. By Theorem A, the Newton polygon $NP(f)$ must contain at least two edges with negative slopes, or one edge of negative slope with more than two lattice points, which is a contradiction.

It is worth mentioning here that Lemma 3 of [1] is indeed equivalent to [17, Lemma 1.4], as proved in [18], and in anticipation of this fact, we comprehend yet another proof of the same. It is interesting to note that revisiting Lemma 1 yielded conspicuous information. The authors observed that in the initial lines of the proof of Subcase I of case I in [1, Lemma 3], the claim

$$\alpha_i \geq \ell;\ \beta_i \geq k - \ell,\ i = 1, \ldots, \kappa, \tag{1}$$

does not hold inevitably as is evident from the following explicit example which per contra

motivates an unprecedented rudimentary proof of the same which is presented in the sequel.

Note that we have $f(x) = f_1(x)f_2(x)$, if we take

$$\begin{aligned} f &= 243 + 243x + 243x^2 + 153x^3 + 33x^4 + 19x^5 + x^6, \\ f_1 &= 9 + 6x + x^2 + x^3, \\ f_2 &= 27 + 9x + 18x^2 + x^3. \end{aligned}$$

Here, $p = 3$, $k = 5$, $j = 3$, $n = 6$, $a_0 = a_1 = a_2 = 243$. We have

$$3^5 \mid 243 = \gcd(a_0, a_1, a_2),\ 3^6 \nmid 243 = a_0,\ \kappa = (j-1)/2 = 1.$$

Further, we have

$$b_0 = 9,\ b_1 = 6,\ b_2 = 1 = b_3;\ c_0 = 27,\ c_1 = 9,\ c_2 = 18,\ c_3 = 1,$$

so that

$$\begin{aligned} \ell &= \alpha_0 = 2,\ \alpha_1 = 1,\ \alpha_2 = 0 = \alpha_3, \\ k - \ell &= \beta_0 = 3,\ \beta_1 = 2,\ \beta_2 = 2,\ \beta_3 = 0. \end{aligned}$$

However, here, we note that

$$\alpha_1 = 1 < 2 = \ell;\ \beta_1 = 2 < 3 = k - \ell.$$

This shows that the Claim (1) in the paper [1] is false although the Lemma 1 itself remains true and does not affect any subsequent results resting on it. This gap in the proof of Lemma 1 in [1] arose due to a computational error due to which a possibility was overlooked which resulted in the aforementioned claim. The proof of Lemma 1 in [1] is inductive, where the claim (1) serves as the first inductive step, which makes the proof irreparable. So, we present a fresh elementary proof of Lemma 1 which does not use any of the arguments of the proof given in the paper [1], and which does not use the Newton polygon.

2. Proof of Lemma 1

We recall from [1] that we may define

$$b_{m+1} = b_{m+2} = \cdots = b_n = 0;\ c_{n-m+1} = c_{n-m+2} = \cdots = c_n = 0,$$

so that we may write

$$a_t = b_0c_t + b_1c_{t-1} + \cdots + b_tc_0,\ \text{for each } t = 0, 1, \ldots, n. \tag{2}$$

It is straightforward to see that for any integers a and b, we have

$$v_p(ab) = v_p(a) + v_p(b);\ v_p(a+b) \geq \min\{v_p(a), v_p(b)\},$$

wherein the inequality becomes an equality if and only if $v_p(a) \neq v_p(b)$. In view of this, we record the following result (which follows inductively) for its later use.

Lemma A. *If $x_1, \ldots, x_s$ is a list of s integers such that minimum of v_p evaluated at $x_1, \ldots, x_s$ occurs at a unique integer x_i in this list, then*

$$v_p(x_1 + \cdots + x_s) = \min\{v_p(x_1), \ldots, v_p(x_s)\} = v_p(x_i).$$

To prove Lemma 1, we first prove the following result.

Lemma 2. *Let $f = f_1 f_2$ where $f = \sum_{i=0}^{n} a_i x^i$, $f_1 = \sum_{i=0}^{m} b_i x^i$, and $f_2 = \sum_{i=0}^{n-m} c_i x^i$ are nonconstant polynomials in $\mathbb{Z}[x]$. Let r and j be positive integers with $r < j \leq n$ such that*

(i) $\gcd(v_p(a_0), j) = 1$,

(ii) $v_p(b_r) = 0$; $v_p(b_i) > 0$ *for* $0 \leq i < r$,

(iii) $v_p(c_{j-r}) = 0$; $v_p(c_i) > 0$ *for* $0 \leq i < j - r$.

Let α and β be the smallest indices for which the following conditions are satisfied

(iv) $v_p(b_\alpha) = \min_{0 \leq i < r} v_p(b_i)$,

(v) $v_p(c_\beta) = \min_{0 \leq i < j-r} v_p(c_i)$,

If $v_p(b_\alpha) = v_p(c_\beta)$ and $r + \beta = j - r + \alpha$, then there exists an index $i < j$ for which $v_p(a_0) > v_p(a_i)$.

Proof. Set $v = v_p$, and let $v(a_0) = k$. By the hypothesis *(ii)* and *(iii)*, we have $v(b_0) > 0$ and $v(c_0) > 0$. Since $a_0 = b_0 c_0$, we have $k = v(a_0) = v(b_0 c_0) = v(b_0) + v(c_0) \geq 2$. Let $v(b_0) = \ell < k$ and $v(c_0) = k - \ell$. We may assume without loss of generality that $\ell \leq k - \ell$. We may also assume that $\alpha > 0$ and $\beta > 0$, since the proof is similar for the case when at least one of α and β is equal to zero. Now we have the following cases.

Case I. $v(b_t) > \frac{r-t}{r-\alpha} v(b_\alpha)$ for all $t = 0, 1, \ldots, \alpha - 1$ and $v(c_s) > \frac{j-r-s}{j-r-\beta} v(c_\beta)$ for all $s = 0, 1, \ldots, \beta - 1$. We will prove the case when $\alpha + \beta > j - r > r$, since the proof is similar for the case when $\alpha + \beta \leq j - r$. To extract the term corresponding to the minimum valuation in the right hand side of (2) for $a_{\alpha+\beta}$, we have decomposed the summand for $a_{\alpha+\beta}$ as follows:

$$a_{\alpha+\beta} = \underbrace{\sum_{i=0}^{\alpha+\beta-j+r} b_i c_{\alpha+\beta-i}}_{\text{I}} + \underbrace{\sum_{i=\alpha+\beta-j+r+1}^{\alpha-1} b_i c_{\alpha+\beta-i}}_{\text{II}} + b_\alpha c_\beta + \underbrace{\sum_{i=\alpha+1}^{r-1} b_i c_{\alpha+\beta-i}}_{\text{III}} + \underbrace{\sum_{i=r}^{\alpha+\beta} b_i c_{\alpha+\beta-i}}_{\text{IV}}. \tag{3}$$

We will show that the $b_\alpha c_\beta$ (the un-grouped term in the right hand side of (3)) is the unique term with the minimum valuation. Using the hypothesis *(iv)* and *(v)* in the summation II of (3), we find that $v(b_i) > v(b_\alpha)$ and $v(c_{\alpha+\beta-i}) \geq v(c_\beta)$ for each $i = \alpha+\beta-j+r+1, \ldots, \alpha-1$. Similarly, in the summation III in (3) we have $v(b_i) \geq v(b_\alpha)$ and $v(c_{\alpha+\beta-i}) > v(c_\beta)$ for each $i = \alpha + 1, \ldots, r - 1$. Consequently, the value of v as evaluated at each term of the summations II and III in (3) is strictly greater than $v(b_\alpha c_\beta)$.

Now turning to the summation I in (3), we use the hypothesis of this case and the given conditions that $v(b_\alpha) = v(c_\beta)$ and $r - \alpha = j - r - \beta$, and arrive at the following:

$$v(b_i) > \frac{r-i}{r-\alpha} v(b_\alpha) \geq \frac{r-(\alpha+\beta-j+r)}{r-\alpha} v(b_\alpha) = 2v(b_\alpha),\ 0 \leq i \leq \alpha+\beta-j+r < \alpha,$$

which shows that $v(b_i c_{\alpha+\beta-i}) > v(b_\alpha c_\beta)$ for each such i. Consequently, the valuation of $b_\alpha c_\beta$ is strictly less than the valuation of each of the term of the summation I in (3).

Finally we consider the summation IV in (3) and use the hypothesis of this case and the given conditions that $v(b_\alpha) = v(c_\beta)$ and $r - \alpha = j - r - \beta$, and get

$$v(c_{\alpha+\beta-i}) > \frac{j-r-(\alpha+\beta-i)}{j-r-\beta} v(c_\beta) \geq \frac{j-r-(\alpha+\beta-r)}{j-r-\beta} v(c_\beta) = 2v(c_\beta),\ r \leq i \leq \alpha+\beta.$$

So, we have $v(b_i c_{\alpha+\beta-i}) > v(b_\alpha c_\beta)$ for each term of the summation IV in (3).

Combining all these observations together and using Lemma A, we arrive at the following:

$$v(a_{\alpha+\beta}) = v(b_\alpha c_\beta) < (1-\alpha/r)\ell + (1-\beta/(j-r))(k-\ell) < k.$$

Case II. $v(b_t) > \frac{r-t}{r-\alpha} v(b_\alpha)$ for all $t = 0, 1, \ldots, \alpha-1$ and $v(c_s) \leq \frac{j-r-s}{j-r-\beta} v(c_\beta)$ for some s with $0 \leq s < \beta$. Let s' be the smallest index with $0 \leq s' < \beta$ for which $v(c_{s'}) \leq \frac{j-r-s'}{j-r-\beta} v(c_\beta)$. Therefore, if $s' > 0$, then we find that

$$v(c_s) > \frac{j-r-s}{j-r-\beta} v(c_\beta) \quad \text{for all } 0 \leq s < s'. \tag{4}$$

Let s^* be the smallest index such that

$$\frac{v(c_{s^*})}{j-r-s^*} = \min_{s' \leq s < \beta} \left\{ \frac{v(c_s)}{j-r-s} \right\}. \tag{5}$$

As before, it will be enough to consider the case when $\alpha + s^* > j - r > r$, since the proof is similar in the other case. Using (2), we have

$$\begin{aligned} a_{\alpha+s^*} = &\underbrace{\sum_{i=0}^{\alpha+s^*-j+r} b_i c_{\alpha+s^*-i}}_{\text{I}} + \underbrace{\sum_{i=\alpha+s^*-j+r+1}^{\alpha+s^*-\beta} b_i c_{\alpha+s^*-i}}_{\text{II}} + \underbrace{\sum_{i=\alpha+s^*-\beta+1}^{\alpha-1} b_i c_{\alpha+s^*-i}}_{\text{III}} \\ &+ b_\alpha c_{s^*} + \underbrace{\sum_{i=\alpha+1}^{\alpha+s^*-s'} b_i c_{\alpha+s^*-i}}_{\text{IV}} + \underbrace{\sum_{i=\alpha+s^*-s'+1}^{r-1} b_i c_{\alpha+s^*-i}}_{\text{V}} + \underbrace{\sum_{i=r}^{\alpha+s^*} b_i c_{\alpha+s^*-i}}_{\text{VI}}. \end{aligned} \tag{6}$$

For each term of the summation I in (6), we use the hypothesis and (5) and find that

$$v(b_i) > \frac{r-i}{r-\alpha} v(b_\alpha) \geq \frac{r-(\alpha+s^*-j+r)}{r-\alpha} v(b_\alpha) = v(b_\alpha) + \frac{j-r-s^*}{j-r-\beta} v(c_\beta) \geq v(b_\alpha) + v(c_{s^*}),$$

for each $i = 0, 1, \ldots, \alpha + s^* - j + r$, which shows that $v(b_i c_{\alpha+s^*-i}) > v(b_\alpha c_{s^*})$ for each term of the summation I in (6).

Considering the terms in the summation II of (6), we have for each index i with $\alpha + s^* - j + r + 1 \leq i \leq \alpha + s^* - \beta$

$$\begin{aligned} v(b_i) + v(c_{\alpha+s^*-i}) &> \frac{r-i}{r-\alpha} v(b_\alpha) + v(c_\beta) \\ &= \frac{r-\alpha+\alpha-i}{r-\alpha} v(b_\alpha) + \frac{j-r-s^*+s^*-\beta}{j-r-\beta} v(c_\beta) \\ &= v(b_\alpha) + \frac{\alpha-i}{r-\alpha} v(b_\alpha) + \frac{j-r-s^*}{j-r-\beta} v(c_\beta) + \frac{s^*-\beta}{j-r-\beta} v(c_\beta) \\ &\geq v(b_\alpha) + v(c_{s^*}) + \frac{\alpha+s^*-i-\beta}{r-\alpha} v(b_\alpha) \geq v(b_\alpha) + v(c_{s^*}), \end{aligned}$$

which shows that the valuation of each term of the summation II in (6) is strictly greater than the valuation of the term $b_\alpha c_{s^*}$. Now consider the summation III in (6). Here, $\alpha + s^* - \beta + 1 \leq i \leq \alpha - 1$ and using (5) we have

$$\begin{aligned} v(b_i) + v(c_{\alpha+s^*-i}) &> \frac{r-i}{r-\alpha} v(b_\alpha) + \frac{j-r-(\alpha+s^*-i)}{j-r-s^*} v(c_{s^*}) \\ &= \frac{r-\alpha+\alpha-i}{r-\alpha} v(b_\alpha) + \frac{j-r-s^*-(\alpha-i)}{j-r-s^*} v(c_{s^*}) \\ &= v(b_\alpha) + \frac{\alpha-i}{r-\alpha} v(b_\alpha) + v(c_{s^*}) - \frac{\alpha-i}{j-r-s^*} v(c_{s^*}) \\ &\geq v(b_\alpha) + \frac{\alpha-i}{j-r-s^*} v(c_{s^*}) + v(c_{s^*}) - \frac{\alpha-i}{j-r-s^*} v(c_{s^*}) = v(b_\alpha) + v(c_{s^*}), \end{aligned}$$

which shows that $v(b_i c_{\alpha+s^*-i}) > v(b_\alpha c_{s^*})$.

Turning to the summation IV in (6), we have for each index i with $\alpha+1 \leq i \leq \alpha+s^*-s'$ using (5) that

$$\begin{aligned} v(b_i) + v(c_{\alpha+s^*-i}) &> v(b_\alpha) + \frac{j-r-(\alpha+s^*-i)}{j-r-s^*} v(c_{s^*}) \\ &= v(b_\alpha) + \frac{j-r-s^*+(i-\alpha)}{j-r-s^*} v(c_{s^*}) \\ &= v(b_\alpha) + v(c_{s^*}) + \frac{i-\alpha}{j-r-s^*} v(c_{s^*}) > v(b_\alpha) + v(c_{s^*}), \end{aligned}$$

which shows that $v(b_i c_{\alpha+s^*-i}) > v(b_\alpha c_{s^*})$ for each such i.

Using the inequality (4) for each term of the summation V in (6), we get

$$\begin{aligned} v(b_i) + v(c_{\alpha+s^*-i}) &> v(b_\alpha) + \frac{j-r-(\alpha+s^*-i)}{j-r-\beta} v(c_\beta) \\ &= v(b_\alpha) + \frac{j-r-s^*+(i-\alpha)}{j-r-\beta} v(c_\beta) \end{aligned}$$

$$= \quad v(b_\alpha) + \frac{j-r-s^*}{j-r-\beta}v(c_\beta) + \frac{i-\alpha}{j-r-\beta}v(c_\beta) > v(b_\alpha c_{s^*}).$$

Finally, in this case we consider the summation VI in (6) for each index i with $r \le i \le \alpha + s^*$. On using (4), we find that

$$\begin{aligned} v(c_{\alpha+s^*-i}) &> \frac{j-r-(\alpha+s^*-i)}{j-r-\beta}v(c_\beta) \\ &\ge \frac{j-r-(\alpha+s^*-r)}{j-r-\beta}v(c_\beta) \\ &= \frac{r-\alpha}{j-r-\beta}v(c_\beta) + \frac{j-r-s^*}{j-r-\beta}v(c_\beta) \ge v(b_\alpha) + v(c_{s^*}), \end{aligned}$$

which shows that $v(b_i c_{\alpha+s^*-i}) > v(b_\alpha c_{s^*})$ for each such i.

Thus, all these observations together conclude that the $b_\alpha c_{s^*}$ is the unique term with minimum valuation in the convolution expression for $a_{\alpha+s^*}$. By Lemma A we have

$$v(a_{\alpha+s^*}) = v(b_\alpha c_{s^*}) = v(b_\alpha) + v(c_{s^*}) < (r-\alpha)\frac{\ell}{r} + (j-r-s^*)\frac{k-\ell}{j-r} < k.$$

Case III. $v(b_t) \le \frac{r-t}{r-\alpha}v(b_\alpha)$ for some t with $0 \le t < \alpha$ and $v(c_s) > \frac{j-r-s}{j-r-\beta}v(c_\beta)$ for all $s = 0, 1, \ldots, \beta-1$. The steps of the proof in this case are parallel to that in the preceding Case II, and we omit the proof.

Case IV. $v(b_t) < \frac{r-t}{r-\alpha}v(b_\alpha)$ for some t with $0 \le t < \alpha$ and $v(c_s) < \frac{j-r-s}{j-r-\beta}v(c_\beta)$ for some s with $0 \le s < \beta$. Let t' and s' be the smallest indices with $0 \le t' < \alpha$ and $0 \le s' < \beta$, for which $v(b_{t'}) < \frac{r-t'}{r-\alpha}v(b_\alpha)$ and $v(c_{s'}) < \frac{j-r-s'}{j-r-\beta}v(c_\beta)$. Therefore, if $t' > 0$ and $s' > 0$, then we have

$$v(b_t) \ge \frac{r-t}{r-\alpha}v(b_\alpha) \text{ for all } 0 \le t < t';\ v(c_s) \ge \frac{j-r-s}{j-r-\beta}v(c_\beta) \text{ for all } 0 \le s < s'. \tag{7}$$

Let t^* and s^* be the smallest indices such that

$$\frac{v(b_{t^*})}{r-t^*} = \min_{t' \le t < \alpha}\left\{\frac{v(b_t)}{r-t}\right\},\ \frac{v(c_{s^*})}{j-r-s^*} = \min_{s' \le s < \beta}\left\{\frac{v(c_s)}{j-r-s}\right\},\ \frac{v(b_{t^*})}{r-t^*} = \frac{v(c_{s^*})}{j-r-s^*}. \tag{8}$$

Again, it will be enough to consider the case when $t^* + s^* > j - r > r$. Using (2), we have

$$\begin{aligned} a_{t^*+s^*} = &\underbrace{\sum_{i=0}^{t^*+s^*-j+r} b_i c_{t^*+s^*-i}}_{\text{I}} + \underbrace{\sum_{i=t^*+s^*-j+r+1}^{t^*+s^*-\beta} b_i c_{t^*+s^*-i}}_{\text{II}} + \underbrace{\sum_{i=t^*+s^*-\beta+1}^{t'-1} b_i c_{t^*+s^*-i}}_{\text{III}} \\ &+ \underbrace{\sum_{i=t'}^{t^*-1} b_i c_{t^*+s^*-i}}_{\text{IV}} + b_{t^*}c_{s^*} + \underbrace{\sum_{i=t^*+1}^{t^*+s^*-s'} b_i c_{t^*+s^*-i}}_{\text{V}} + \underbrace{\sum_{i=t^*+s^*-s'+1}^{\alpha-1} b_i c_{t^*+s^*-i}}_{\text{VI}} \\ &+ \underbrace{\sum_{i=\alpha}^{r-1} b_i c_{t^*+s^*-i}}_{\text{VII}} + \underbrace{\sum_{i=r}^{t^*+s^*} b_i c_{t^*+s^*-i}}_{\text{VIII}}. \end{aligned} \tag{9}$$

Here, we will show that $b_{t^*}c_{s^*}$ is the unique term of minimum valuation in the convolution expression for $a_{t^*+s^*}$.

Considering the indices of the summation I in (9) we have for each index i with $0 \leq i \leq t^* + s^* - j + r < t'$ on using the inequality (7) that

$$\begin{aligned} v(b_i) &\geq \frac{r-i}{r-\alpha}v(b_\alpha) \\ &\geq \frac{r-(t^*+s^*-j+r)}{r-\alpha}v(b_\alpha) \\ &= \frac{r-t^*}{r-\alpha}v(b_\alpha) + \frac{j-r-s^*}{j-r-\beta}v(c_\beta) > v(b_{t^*}) + v(c_{s^*}). \end{aligned}$$

This shows that $v(b_i c_{t^*+s^*-i}) > v(b_{t^*}c_{s^*})$ for each term of the summation I in (9).

For each term of the summation II in (9), we have

$$\begin{aligned} v(b_i) + v(c_{t^*+s^*-i}) &\geq \frac{r-i}{r-\alpha}v(b_\alpha) + v(c_\beta) \\ &= \frac{r-t^*+t^*-i}{r-\alpha}v(b_\alpha) + \frac{j-r-s^*+s^*-\beta}{j-r-\beta}v(c_\beta) \\ &= \frac{r-t^*}{r-\alpha}v(b_\alpha) + \frac{j-r-s^*}{j-r-\beta}v(c_\beta) + \frac{t^*+s^*-\beta-i}{r-\alpha}v(b_\alpha) \\ &> v(b_{t^*}c_{s^*}), \end{aligned}$$

for each index $i = t^* + s^* - j + r + 1 \leq i \leq t^* + s^* - \beta$.

For $t^* + s^* - \beta + 1 \leq i \leq t' - 1$ (indices in the summation III of (9)) we use (7) and (8) and we have the following:

$$\begin{aligned} v(b_i) + v(c_{t^*+s^*-i}) &\geq \frac{r-i}{r-\alpha}v(b_\alpha) + \frac{j-r-(t^*+s^*-i)}{j-r-s^*}v(c_{s^*}) \\ &= \frac{r-t^*+t^*-i}{r-\alpha}v(b_\alpha) + \frac{j-r-s^*-(t^*-i)}{j-r-s^*}v(c_{s^*}) \\ &> v(b_{t^*}) + \frac{t^*-i}{r-\alpha}v(b_\alpha) + v(c_{s^*}) - \frac{t^*-i}{j-r-s^*}v(c_{s^*}) \\ &> v(b_{t^*}) + \frac{t^*-i}{j-r-s^*}v(c_{s^*}) + v(c_{s^*}) - \frac{t^*-i}{j-r-s^*}v(c_{s^*}) \\ &= v(b_{t^*}c_{s^*}), \end{aligned}$$

which shows that $v(b_i c_{t^*+s^*-i}) > v(b_{t^*}c_{s^*})$ for each term of the summation III in (9).

For each index i corresponding to the indices in the summations IV and V in (9), we find that we have

$$\begin{aligned} v(b_i) + v(c_{t^*+s^*-i}) &> \frac{r-i}{r-t^*}v(b_{t^*}) + \frac{j-r-(t^*+s^*-i)}{j-r-s^*}v(c_{s^*}) \\ &= \frac{r-t^*+t^*-i}{r-t^*}v(b_{t^*}) + \frac{j-r-s^*+(i-t^*)}{j-r-s^*}v(c_{s^*}) \end{aligned}$$

$$= \quad v(b_{t^*}) - \frac{i-t^*}{r-t^*}v(b_{t^*}) + v(c_{s^*}) + \frac{i-t^*}{j-r-s^*}v(c_{s^*}) = v(b_{t^*}c_{s^*}).$$

Turning to the summation VI in (9), we have for each index i with $t^* + s^* - s' + 1 \leq i \leq \alpha - 1$ that

$$\begin{aligned} v(b_i) + v(c_{t^*+s^*-i}) &\geq \frac{r-i}{r-t^*}v(b_{t^*}) + \frac{j-r-(t^*+s^*-i)}{j-r-\beta}v(c_\beta) \\ &= \frac{r-t^*+t^*-i}{r-t^*}v(b_{t^*}) + \frac{j-r-s^*-(t^*-i)}{j-r-\beta}v(c_\beta) \\ &> v(b_{t^*}) - \frac{i-t^*}{r-t^*}v(b_{t^*}) + v(c_{s^*}) + \frac{i-t^*}{j-r-\beta}v(c_\beta) \\ &> v(b_{t^*}) - \frac{i-t^*}{r-t^*}v(b_{t^*}) + v(c_{s^*}) + \frac{i-t^*}{r-t^*}v(b_{t^*}) = v(b_{t^*}) + v(c_{s^*}), \end{aligned}$$

which implies $v(b_i c_{t^*+s^*-i}) > v(b_{t^*}c_{s^*})$ for each such i.

For each index corresponding to the indices in the summation VII in (9), we find that

$$\begin{aligned} v(b_i) + v(c_{t^*+s^*-i}) &\geq v(b_\alpha) + \frac{j-r-(t^*+s^*-i)}{j-r-\beta}v(c_\beta) \\ &= \frac{r-t^*+t^*-\alpha}{r-\alpha}v(b_\alpha) + \frac{j-r-s^*-(t^*-i)}{j-r-\beta}v(c_\beta) \\ &= \frac{r-t^*}{r-\alpha}v(b_\alpha) + \frac{j-r-s^*}{j-r-\beta}v(c_\beta) + \frac{i-\alpha}{r-\alpha}v(b_\alpha) > v(b_{t^*}c_{s^*}). \end{aligned}$$

Finally, for each index i with $r \leq i \leq t^* + s^*$ in the summation VIII in (9) we have

$$\begin{aligned} v(c_{t^*+s^*-i}) &\geq \frac{j-r-(t^*+s^*-i)}{j-r-\beta}v(c_\beta) \\ &\geq \frac{j-r-(t^*+s^*-r)}{j-r-\beta}v(c_\beta) \\ &= \frac{r-t^*}{r-\alpha}v(b_\alpha) + \frac{j-r-s^*}{j-r-\beta}v(c_\beta) > v(b_{t^*}) + v(c_{s^*}), \end{aligned}$$

which shows that $v(b_i c_{t^*+s^*-i}) > v(b_{t^*}c_{s^*})$ for each such i.

Combining all these observations together concludes that $b_{t^*}c_{s^*}$ is the unique term of minimum valuation in the convolution expression for $a_{t^*+s^*}$. By Lemma A, the assumption of this case and the hypotheses that $v(b_\alpha) = v(c_\beta)$ and $r - \alpha = j - r - \beta$, we find that $v(a_{t^*+s^*}) = v(b_{t^*}c_{s^*}) < k$.

It remains to prove the case when the assumption made in the third equality in (8) is replaced by the inequality $v(b_{t^*})/(r-t^*) < v(c_{s^*})/(j-r-s^*)$ keeping the rest of all conditions unchanged. In this case, proceeding with calculations similar to the earlier ones, we find that $b_{t^*}c_{j-r}$ is the unique term of minimum valuation in the convolution expression for a_{t^*+j-r}. Consequently, by Lemma A, we have $v(a_{t^*+j-r}) = v(b_{t^*}c_{j-r}) = v(b_{t^*}) < k$. On the other hand, if the assumption made in the third equality in (8) is replaced by

the inequality $v(b_{t^*})/(r-t^*) > v(c_{s^*})/(j-r-s^*)$, then the unique term of minimal valuation in the convolution expression for a_{r+s^*} is $b_r c_{s^*}$, and again by Lemma A we have $v(a_{r+s^*}) = v(b_r c_{s^*}) = v(c_{s^*}) < k$.

We observe that either $v(b_0) \neq \frac{r}{r-\alpha} v(b_\alpha)$, or $v(c_0) \neq \frac{j-r}{j-r-\beta} v(c_\beta)$. To see this, we suppose on the contrary that $v(b_0) = \frac{r}{r-\alpha} v(b_\alpha)$ and $v(c_0) = \frac{j-r}{j-r-\beta} v(c_\beta)$. Consequently, using the hypothesis that $v(b_\alpha) = v(c_\beta)$, $r-\alpha = j-r-\beta$, we have $k = v(b_0) + v(c_0) = \frac{r}{r-\alpha} v(b_\alpha) + \frac{j-r}{j-r-\beta} v(c_\beta) = \frac{v(b_\alpha)}{r-\alpha} j = \ell j/r$, which is impossible since $\gcd(k, j) = 1$ and $r < j$.

We will make use of Lemma 2 in the proof of Lemma 1 as follows.

Proof. Proof of Lemma 1] Set $v = v_p$. From $a_0 = b_0 c_0$, we have $v(a_0) = v(b_0) + v(c_0)$. Let $v(b_0) = \ell$ and $v(c_0) = k - \ell$ with $1 \leq \ell \leq k-1$. By the hypothesis, all coefficients a_i, $0 \leq i \leq j-1$ satisfy $v(a_i) \geq k$. We may assume without loss of generality that $\ell \leq k - \ell$. If p divides b_i for all $i = 0, 1, \ldots, j-1$, then p divides the sum $b_0 c_j + \cdots + b_{j-1} c_1 + b_j c_0 = a_j$ and we are done. So, let us assume that there exists a smallest index $r < j$ for which p does not divide b_r. Thus $v(b_i) > 0$ for each $i = 0, \ldots, r-1$ and $v(b_r) = 0$. Assume on the contrary that p does not divide a_j, that is, $v(a_j) = 0$.

Applying the convolution identity (2) to indices $r+i$, we isolate the term $b_r c_i$ and determine the valuation structure needed to locate the minimal term. In view of this we find recursively that p divides the sum

$$a_{r+i} - (b_0 c_{r+i} + b_1 c_{r+i-1} + \cdots + b_{r-1} c_{i+1}) - (b_{r+1} c_{i-1} + \cdots + b_{r+i} c_0) = b_r c_i,$$

so that p divides $b_r c_i$ for each $i = 1, \ldots, j-r-1$. This in view of the fact that $v(b_r) = 0$ tells us that $v(c_i) > 0$ for each $i = 0, \ldots, j-r-1$. Consequently p divides each of $(b_0 c_j + \cdots + b_{r-1} c_{j-r+1})$ and $(b_{r+1} c_{j-r-1} + \cdots + b_j c_0)$ and thus p divides their sum, which from (2) is equal to $a_j - b_r c_{j-r}$. Since $v(a_j) = 0$, it follows that $v(b_r c_{j-r}) = 0$, which proves that $v(c_{j-r}) = 0$.

Let α and β be the smallest indices for which

$$v(b_\alpha) = \min_{0 \leq i < r} v(b_i), \quad v(c_\beta) = \min_{0 \leq i < j-r} v(c_i).$$

We may assume that $\alpha > 0$ and $\beta > 0$, since the proof is similar for the case when at least one of α and β is equal to zero. Now we have the following cases.

Case I. $v(b_\alpha) \neq v(c_\beta)$. First assume that $v(b_\alpha) < v(c_\beta)$. In this case, we have $v(b_\alpha) < v(c_\beta) \leq v(c_i)$ for all $i = 0, \ldots, j-r-1$, and since $v(b_\alpha) < v(b_t)$ for all $t = 0, \ldots, \alpha-1$, we find that $v(b_\alpha c_{j-r}) < v(b_i c_t)$ for all such i and t. Consequently, $b_\alpha c_{j-r}$ is the unique term in the sum $b_0 c_{j-r+\alpha} + \cdots + b_{j-r+\alpha} c_0 = a_{j-r+\alpha}$ for which $\min\{v(b_0 c_{j-r+\alpha}), \ldots, v(b_{j-r+\alpha} c_0)\} = v(b_\alpha c_{j-r}) = v(b_\alpha)$, where we note that $j - r + \alpha < j$. Consequently, by Lemma A, we have

$$k \leq v(a_{j-r+\alpha}) = \min\{v(b_0 c_{j-r+\alpha}), \ldots, v(b_{j-r+\alpha} c_0)\} \quad = \quad v(b_\alpha c_{j-r}) = v(b_\alpha) \leq \ell < k,$$

which is a contradiction.

Similarly, if $v(b_\alpha) > v(c_\beta)$, then we have $b_r c_\beta$ is the unique term in the sum $b_0 c_{r+\beta} + \cdots + b_{r+\beta} c_0 = a_{r+\beta}$ for which $\min\{v(b_0 c_{r+\beta}), \ldots, v(b_{r+\beta} c_0)\} = v(b_r c_\beta)$, where $r + \beta < j$, and by Lemma A, $k \leq v(a_{r+\beta}) = v(b_r c_\beta) = v(c_\beta) < v(b_\alpha) \leq \ell < k$, which is a contradiction.

Case II. $v(b_\alpha) = v(c_\beta)$ and $j - r + \alpha \neq r + \beta$. In this case, we may assume without loss of generality that $r < j - r$, since the proof for the case when $j - r \leq r$ is similar. First assume that $j - r + \alpha < r + \beta$. Using (2), we get

$$a_{j-r+\alpha} = \underbrace{\sum_{i=0}^{\alpha-1} b_i c_{j-r+\alpha-i}}_{\text{I}} + b_\alpha c_{j-r} + \underbrace{\sum_{i=\alpha+1}^{j-r+\alpha-\beta} b_i c_{j-r+\alpha-i}}_{\text{II}} + \underbrace{\sum_{i=j-r+\alpha-\beta+1}^{j-r+\alpha} b_i c_{j-r+\alpha-i}}_{\text{III}} \quad (10)$$

Since $v(b_\alpha) < v(b_t)$ for every $t = 0, \ldots, \alpha - 1$, and $v(b_\alpha) = v(c_\beta) < v(c_s)$ for every $s = 0, \ldots, \beta - 1$, it follows that $v(b_\alpha c_{j-r}) < v(b_t c_s)$ for all such indices t and s. Consequently, the value of v as evaluated at each term of the summations I and III in (10) is strictly greater than $v(b_\alpha c_{j-r})$. Further, $v(b_\alpha) = v(c_\beta) \leq v(c_s)$ for each $s = \beta, \beta + 1, \ldots, j - r - 1$, and since $j - r + \alpha - \beta < r$, we have $v(b_i) > 0$ for each $i = \alpha + 1, \ldots, j - r + \alpha - \beta$. We find that the value of v as evaluated at each term of the summation II in (10) strictly exceeds the value $v(b_\alpha) = v(b_\alpha c_{j-r})$. These observations together conclude that the minimum over the values of v evaluated at each term in the expression for $a_{j-r+\alpha}$ occurs exactly at the unique term $b_\alpha c_{j-r}$. This in view of Lemma A proves that

$$k \leq v(a_{j-r+\alpha}) = \min\{v(b_0 c_{j-r+\alpha}), \ldots, v(b_{j-r+\alpha} c_0)\} = v(b_\alpha c_{j-r}) = v(b_\alpha) \leq \ell < k,$$

which is a contradiction.

Similarly, if $j - r + \alpha > r + \beta$, then we have that the minimum over the values of v evaluated at each term in the expression for $a_{r+\beta}$ occurs exactly at the unique term $b_r c_\beta$. This on using Lemma A gives

$$k \leq v(a_{r+\beta}) = \min\{v(b_0 c_{r+\beta}), \ldots, v(b_{r+\beta} c_0)\} = v(b_r c_\beta) = v(c_\beta) = v(b_\alpha) \leq \ell < k,$$

which is a contradiction.

Case III. $v(b_\alpha) = v(c_\beta)$ and $j - r + \alpha = r + \beta$. In this case, we use Lemma 2 to deduce that there exists an index $i < j$ for which $v(a_i) < k = v(a_0)$, which is a contradiction, since $v(a_i) \geq k$ for each $i < j$.

Acknowledgements

The authors are grateful to the anonymous referees for valuable suggestions that improved the presentation of the paper.

Senior Research Fellowship (SRF) to Ms. Rishu Garg wide grant no. CSIRAWARD/JRF-NET2022/11769 from Council of Scientific and Industrial Research (CSIR) is gratefully acknowledged. The present paper is a part of her Ph.D. thesis work.

Disclosure statement

The authors report that there are no competing interests to declare.

References

[1] Jitender Singh and Sanjeev Kumar. A new class of irreducible polynomials. *Commun. Algebra*, 49(6):2722–2727, June 2021.

[2] L Schönemann. Von denjenigen moduln, welche potenzen von primzahlen sind.(fortsetzung). *J. Reine Angew. Math.*, 1846(32):93–105, July 1846.

[3] G Eisenstein. Über die irreductibilität und einige andere eigenschaften der gleichung, von welcher die theilung der ganzen lemniscate abhängt. *J. Reine Angew. Math.*, 1850(39):160–179, January 1850.

[4] G Dumas. Sur quelques cas d'irréductibilité des polynomes à coefficients rationnels. *Journal de Mathématiques Pures et Appliquées*, 2:191–258, 1906.

[5] M Ram Murty. Prime numbers and irreducible polynomials. *Am. Math. Mon.*, 109(5):452–458, May 2002.

[6] Jitender Singh. Prime numbers and factorization of polynomials. *Indian J Pure Appl Math*, January 2026. https://doi.org/10.1007/s13226-026-00920-y.

[7] Sanjeev Kumar and Jitender Singh. A study of some recent irreducibility criteria for polynomials having integer coefficients. *arXiv Preprint:https://arxiv.org/abs/2310.02860*, pages 1–20, October 2023.

[8] Weilin Zhang and Pingzhi Yuan. On two conjectures of irreducible polynomials. *Commun. Algebra*, 51(11):4879–4884, November 2023.

[9] Kurt Girstmair. On an irreducibility criterion of m. ram murty. *Am. Math. Mon.*, 112(3):269–270, March 2005.

[10] Jitender Singh and Sanjeev Kumar. A note on girstmair's irreducibility criterion. *Bull. Aust. Math. Soc.*, 106(1):62–66, August 2022.

[11] Jitender Singh and Rishu Garg. Some factorization results on polynomials having integer coefficients. *Commun. Algebra*, 52(6):2467–2474, June 2024.

[12] Jitender Singh. A generalization of dumas irreducibility criterion. *arXiv Preprint: https://arxiv.org/abs/2505.08549*, pages 1–10, December 2025.

[13] L Schönemann. Von denjenigen moduln, welche potenzen von primzahlen sind.(fortsetzung). *J. Reine Angew. Math.*, 1846(32):93–105, July 1846.

[14] Rishu Garg, Jitender Singh, and Sanjeev Kumar. Further generalizations of girstmair's irreducibility criterion. *Arch. Math.*, 125(6):589–597, December 2025.

[15] Rishu Garg and Jitender Singh. On irreducible factors of polynomials over integers. *arXiv Preprint: https://arxiv.org/abs/2512.20262*, pages 1–14, December 2025.

[16] Nicolae Ciprian Bonciocat. Schönemann–Eisenstein–Dumas-type irreducibility conditions that use arbitrarily many prime numbers. *Commun. Algebra*, 43(8):3102–3122, August 2015.

[17] Nicolae Ciprian Bonciocat, Yann Bugeaud, Mihai Cipu, and Maurice Mignotte. Irreducibility criteria for sums of two relatively prime polynomials. *Int. J. Number Theory*, 09(06):1529–1539, September 2013.

[18] Jitender Singh and Sanjeev Kumar. Irreducibility via location of zeros. *arXiv Preprint: https://arxiv.org/abs/2309.08502*, pages 1–8, September 2023.