

Arithmetic in the ring of formal power series with integer coefficients

Daniel Birmajer and Juan B. Gil

1 INTRODUCTION

The divisibility and factorization theory of the integers and of the ring of polynomials (in one variable) over the integers are standard topics in a first course in abstract algebra. Concepts such as prime, irreducible, and invertible elements, unique factorization, and irreducibility criteria are extensively studied and are part of the core of the course. On the other hand, the natural extension of the ring of polynomials $R[x]$ over R , namely the ring $R[[x]]$ of formal power series in one variable over R , is hardly ever mentioned in such a course. In most cases, it is relegated to the homework problems (or to the exercises in the textbooks), and one learns that, like $R[x]$, $R[[x]]$ is an integral domain provided that R is an integral domain. More surprising is to learn that, in contrast to the situation of polynomials, in $R[[x]]$ there are many invertible elements: while the only units in $R[x]$ are the units of R , a necessary and sufficient condition for a power series to be invertible is that its constant term be invertible in R . This fact makes the study of arithmetic in $R[[x]]$ simple when R is a field: the only prime element is the variable x . As might be expected, the study of prime factorization in $\mathbb{Z}[[x]]$ is much more interesting (and complicated), but to the best of our knowledge it is not treated in detail in the available literature.

After some basic considerations, it is apparent that the question of deciding whether or not an integral power series is prime is a difficult one, and it seems worthwhile to develop criteria to determine irreducibility in $\mathbb{Z}[[x]]$ similar to Eisenstein's criterion for polynomials. In this note we propose an easy argument that provides us with an infinite class of irreducible power series over \mathbb{Z} . As in the case of Eisenstein's criterion in $\mathbb{Z}[x]$, our criteria give only sufficient conditions, and the question of whether or not a given power series is irreducible remains open in a vast array of cases, including quadratic polynomials.

It is important to note that irreducibility in $\mathbb{Z}[x]$ and in $\mathbb{Z}[[x]]$ are, in general, unrelated. For instance, $6 + x + x^2$ is irreducible in $\mathbb{Z}[x]$ but can be factored in $\mathbb{Z}[[x]]$, while $2 + 7x + 3x^2$ is irreducible in $\mathbb{Z}[[x]]$ but equals $(2 + x)(1 + 3x)$ as a polynomial (observe that this is not a proper factorization in $\mathbb{Z}[[x]]$ since $1 + 3x$ is invertible). For some particular quadratic polynomials we are able to answer the question of irreducibility, but we leave (among many others) some questions for further research: Is there a definite criterion to decide whether a quadratic

polynomial is irreducible in $\mathbb{Z}[[x]]$? Is there an algorithmic method that decides this question in a finite number of steps? If so, what is its complexity? In order to get acquainted with the difficulty of these questions, we encourage the reader to analyze the simple polynomial $a(x) = 4 + 4x + \alpha x^2$ with $\alpha \in \mathbb{Z}$. Obviously, $a(x)$ is reducible when α is an even number, and it can be easily seen to be irreducible when $\alpha \equiv 3 \pmod{4}$. However, if $\alpha \equiv 1 \pmod{4}$, the situation is more complicated except when $\alpha = 1$ (in which case $a(x)$ factors as $(2 + x)^2$). Using a computer algebra system (such as MAPLE), one can prove that the polynomial $4 + 4x + \alpha x^2$ is irreducible in $\mathbb{Z}[[x]]$ when $\alpha \equiv 5$ or $9 \pmod{16}$, and with some extra effort, one can also check that $a(x)$ is irreducible for $\alpha \equiv 13 \pmod{32}$ and for $\alpha = 17$. On the other hand, it can be shown that the polynomial $4 + 4x + 29x^2$ is reducible as a power series.

We finish this introduction mentioning that all the above discussion makes sense because the ring $\mathbb{Z}[[x]]$ is a unique factorization domain (UFD). This fact is by no means as well known as the fact that $\mathbb{Z}[x]$ is a UFD, and its proof is not found in most of the introductory abstract algebra textbooks. Again, the situation here is different from that in $\mathbb{Z}[x]$: it is known that $R[x]$ is a UFD when R is a UFD, but it was shown by Samuel in [6] that it is possible for $R[[x]]$ not to be a UFD even if R is one. On the bright side, if R is a principal ideal domain (PID), then $R[[x]]$ is a UFD. This is the reason why our object of study, $\mathbb{Z}[[x]]$, is indeed a UFD. In fact, many of the results in this article also work for other familiar PIDs such as the Gaussian integers.

In the hope that this note may be used as a basis for further exploration of the subject, and for the reader's convenience, we have made the article self-contained and strived to make it accessible to anyone with a little background in abstract algebra. Our proof that $\mathbb{Z}[[x]]$ is a UFD follows the guidelines of [5]. For a more extensive treatment of the conditions that might be imposed on R in order for $R[[x]]$ to be a UFD, the reader is referred to [2], [4], and [7].

2 INTEGRAL DOMAINS

An integral domain D is a commutative ring with $1 \neq 0$ and the property that $ab = 0$ implies $a = 0$ or $b = 0$ for all $a, b \in D$.

Definition 2.1 Let D be an integral domain.

- (a) An element $u \in D$ is called a *unit* if there exists $v \in D$ such that $uv = 1$.
- (b) Suppose $r \in D$ is nonzero and is not a unit. Then r is called *irreducible* in D if $r = ab$ implies a or b is a unit. Otherwise r is said to be *reducible*.
- (c) A nonzero element p is said to be *prime* if it is not a unit and $p \mid ab$ implies $p \mid a$ or $p \mid b$ for all $a, b \in D$.
- (d) Two elements a and b of D such that $a = ub$ for some unit $u \in D$ are said to be *associate* in D .

(e) We say that D is a *unique factorization domain* (UFD), or simply that D is *factorial*, if every nonzero element $m \in D$ which is not a unit can be written as a (finite) product of irreducible elements. Moreover, this factorization is unique in the following sense: If $m = t_1 \cdots t_k$ and $m = s_1 \cdots s_j$ are two factorizations of m into irreducibles, then $k = j$ and there is a permutation σ of $\{1, \dots, k\}$ such that t_i and $s_{\sigma(i)}$ are associates for $1 \leq i \leq k$.

Proposition 2.2 *If $p \in D$ is prime, then p is irreducible.*

Proof. Assume that $p = ab$. Since p is prime, we have $p \mid a$ or $p \mid b$, say $p \mid a$. Then $p = ab = pqb$ for some $q \in D$, and so $p(1 - qb) = 0$. Since D is an integral domain and p is not zero, we have that $1 = qb$, that is, b is a unit. \square

Proposition 2.3 *If D is a UFD and $p \in D$ is irreducible, then p is prime.*

Proof. Let D be a UFD and $p \in D$ irreducible. Suppose that $p \mid ab$. Write a and b as finite products of irreducibles. The product of these two factorizations is the unique (up to associates) factorization of ab . Since $p \mid ab$, it follows that p is associate with at least one of the irreducible elements in the factorization of ab , implying that $p \mid a$ or $p \mid b$. \square

3 POWER SERIES

Let D be an integral domain. The set $D[[x]]$ of formal power series in the indeterminate x over D is defined to be the set of all formal infinite sums

$$\sum_{n=0}^{\infty} a_n x^n = a_0 + a_1 x + a_2 x^2 + a_3 x^3 + \cdots$$

with $a_j \in D$ for all $j = 0, 1, 2, \dots$

Addition and multiplication of power series are defined by extending the usual addition and multiplication rules for polynomials, namely, term-by-term addition

$$\sum_{n=0}^{\infty} a_n x^n + \sum_{n=0}^{\infty} b_n x^n = \sum_{n=0}^{\infty} (a_n + b_n) x^n,$$

and the Cauchy product

$$\left(\sum_{n=0}^{\infty} a_n x^n \right) \times \left(\sum_{n=0}^{\infty} b_n x^n \right) = \sum_{n=0}^{\infty} \left(\sum_{k=0}^n a_k b_{n-k} \right) x^n.$$

Provided with these two operations, $D[[x]]$ is an integral domain – a commutative ring with identity $1 \neq 0$ and no zero divisors.

Proposition 3.1 *A formal power series $a(x) = \sum a_n x^n \in D[[x]]$ is invertible if and only if a_0 is invertible in D .*

Proof. If $a(x)$ is a unit in $D[[x]]$, there exists $b(x) \in D[[x]]$ such that $a(x)b(x) = 1$. In particular, $a_0b_0 = 1$, and so a_0 is a unit in D .

Conversely, assume that a_0 is a unit in D . In order for $a(x)$ to be invertible, we must find $b(x) = \sum b_jx^j \in D[[x]]$ satisfying the relation $a(x)b(x) = 1$. Thus the following (infinite) system of equations must hold:

$$\begin{aligned} 1 &= a_0b_0 \\ 0 &= a_0b_1 + a_1b_0 \\ 0 &= a_0b_2 + a_1b_1 + a_2b_0 \\ &\vdots \\ 0 &= a_0b_n + \sum_{j=1}^n a_jb_{n-j} \\ &\vdots \end{aligned}$$

If we define inductively

$$\begin{aligned} b_0 &= a_0^{-1}, \\ b_n &= -a_0^{-1} \sum_{j=1}^n a_jb_{n-j} \quad \text{for } n = 1, 2, \dots, \end{aligned}$$

we get $a(x)b(x) = 1$, thus $a(x)$ is indeed a unit. \square

Proposition 3.2 *If p is prime in D , then p is prime in $D[[x]]$.*

Proof. Let $c(x) = a(x)b(x)$ with $a(x), b(x) \in D[[x]]$. Assume that $p \mid c(x)$ but p does not divide $b(x)$. Let m be the smallest power of x such that p does not divide the coefficient b_m . Since $c_m = a_0b_m + \sum_{j=1}^m a_jb_{m-j}$, and since $p \mid c_m$ and $p \mid \sum_{j=1}^m a_jb_{m-j}$, we conclude that $p \mid a_0$. By induction, suppose that p divides a_j for all $j < k$. Now, the coefficient $c_{m+k} = \sum_{j=0}^{m+k} a_jb_{m+k-j}$ can be conveniently rearranged as

$$c_{m+k} = a_kb_m + \sum_{\substack{i+j=m+k \\ i < k}} a_ib_j + \sum_{\substack{i+j=m+k \\ j < m}} a_ib_j.$$

By our hypotheses, $p \mid c_{m+k}$, $p \mid a_i$ for all $i < k$, and $p \mid b_j$ for all $j < m$. Therefore, $p \mid a_kb_m$ and thus $p \mid a_k$. In conclusion, p must divide $a(x)$. \square

Here is an easy criterion to find irreducible elements in $D[[x]]$.

Proposition 3.3 *If a_0 is prime, then $a(x)$ is irreducible.*

Proof. Let $a(x) = p(x)q(x)$ with $p(x), q(x) \in D[[x]]$. In particular, $a_0 = p_0q_0$. Since a_0 is prime, it follows that either p_0 or q_0 is a unit in D , so either $p(x)$ or $q(x)$ is invertible in $D[[x]]$. \square

We now focus on the case when $D = \mathbb{Z}$, the set of integer numbers.

Proposition 3.4 *Let $a(x) \in \mathbb{Z}[[x]]$ be a non-invertible element. If a_0 is not a prime power, then $a(x)$ is reducible.*

Proof. We will find power series $p(x) = \sum p_n x^n$ and $q(x) = \sum q_n x^n$ in $\mathbb{Z}[[x]]$ such that $a(x) = p(x)q(x)$.

First of all, recall that as a consequence of the Euclidean algorithm for finding the greatest common divisor $\gcd(m, n)$ of two integers m and n , one can find (infinitely many) integers α and β such that $\gcd(m, n) = m\alpha + n\beta$.

Since a_0 is not a prime power, it can be written as the product of two non-invertible integers, say $a_0 = mn$, with $\gcd(m, n) = 1$. Let $\alpha, \beta \in \mathbb{Z}$ be such that $1 = m\alpha + n\beta$. Then $a(x)$ can be factored by means of the following inductive algorithm. Let $p_0 = m$ and $q_0 = n$. Since $a_1 = m\alpha a_1 + n\beta a_1$, if we set

$$p_1 = \beta a_1 \quad \text{and} \quad q_1 = \alpha a_1,$$

then we get $a_1 = p_0 q_1 + p_1 q_0$, as desired. Once $p_0, q_0, p_1,$ and q_1 are defined, we can solve $a_2 = p_0 q_2 + p_1 q_1 + p_2 q_0$, or equivalently,

$$a_2 - p_1 q_1 = p_0 q_2 + p_2 q_0 = m q_2 + n p_2,$$

by using again the relation $1 = m\alpha + n\beta$ and setting

$$p_2 = \beta(a_2 - p_1 q_1) \quad \text{and} \quad q_2 = \alpha(a_2 - p_1 q_1).$$

For $j = 3, 4, 5, \dots$, we proceed inductively and define

$$p_j = \beta \left(a_j - \sum_{k=1}^{j-1} p_k q_{j-k} \right) \quad \text{and} \quad q_j = \alpha \left(a_j - \sum_{k=1}^{j-1} p_k q_{j-k} \right).$$

With these coefficients, we obtain the desired factorization $a(x) = p(x)q(x)$. \square

In the remaining part of this section we will prove that $\mathbb{Z}[[x]]$ is a unique factorization domain. As mentioned in the introduction, this fact does not appear explicitly in most introductory algebra books. For this reason, we give here a complete proof following ideas from the book by Kaplansky [5].

The central result of this section is Theorem 3.7, which will be proven with the help of the following two propositions.

Proposition 3.5 *If every non-invertible nonzero element of an integral domain R can be written as a (finite) product of primes, then R is a UFD.*

Proof. Since every prime is irreducible, we only need to prove uniqueness of the factorization. Let $m \in R$ be nonzero and non-invertible, and suppose that $m = t_1 \cdots t_k$ and $m = s_1 \cdots s_j$ are two factorizations of m into irreducible elements. Since t_1 is prime, we have (after rearranging the factors, if necessary) that $t_1 \mid s_1$, which implies that t_1 is associate to s_1 . Since R is a domain, we obtain that $t_2 \cdots t_k$ and $s_2 \cdots s_j$ are associates, and by induction in k we conclude that $k = j$ and that s_2, \dots, s_j is a permutation of associates of t_2, \dots, t_k . Thus uniqueness follows. \square

Proposition 3.6 (Krull) *Let S be a nonempty multiplicatively closed set that does not contain 0 in a ring R , and let I be an ideal in R maximal with respect to the property that $I \cap S = \emptyset$. Then I is prime in R .*

Proof. Recall that an ideal P is prime if it is proper and $ab \in P$ implies $a \in P$ or $b \in P$. Let I be an ideal of R maximal with respect to the property that $I \cap S = \emptyset$. Suppose that I is not prime. Then there exist $a, b \in R$ such that $a \notin I$ and $b \notin I$, but $ab \in I$. The ideal (I, a) is larger than I and so $(I, a) \cap S$ is not empty. Take $s \in S$ such that $s = m + xa$, with $m \in I$ and $x \in R$. Similarly, we can find $t \in S$ such that $t = n + yb$, with $n \in I$ and $y \in R$. Then $st = mn + mya + nxa + abxy \in I$, hence $st \notin S$, which implies that S is not multiplicatively closed. \square

Theorem 3.7 *An integral domain R is a UFD if and only if every nonzero prime ideal P in R contains a prime element.*

Proof. Let R be a UFD and P a nonzero prime ideal. Then P contains an element a that is neither 0 nor a unit. When a is factored as a product of primes $a = p_1 \cdots p_t$, one of the factors must be contained in P .

Conversely, assume that every nonzero prime ideal in R contains a prime element. Let S denote the set that consists of all products of prime elements and all units. Clearly, S is a multiplicatively closed set not containing 0. Moreover, it can be easily shown by induction that if $ab \in S$, then a and b both lie in S .

By Proposition 3.5, it suffices to show that S contains all nonzero elements of R . Let c be such an element of R . If we suppose that $c \notin S$, then the principal ideal generated by c is disjoint from S . By Zorn's lemma, c is contained in an ideal that is maximal with respect to the property of being disjoint from S . By Proposition 3.6 this ideal is prime and must contain a prime element; a contradiction. Thus $c \in S$ and R is a UFD. \square

Theorem 3.8 *The ring $\mathbb{Z}[[x]]$ is a UFD.*

Proof. We will show that every nonzero prime ideal in $\mathbb{Z}[[x]]$ is generated either by x , or by p and x with p prime, or by $a(x)$ with $a(x)$ prime. Hence every nonzero prime ideal in $\mathbb{Z}[[x]]$ contains a prime element, and therefore the statement of the theorem is a direct consequence of Theorem 3.7 with $R = \mathbb{Z}[[x]]$.

Let P be a prime ideal in $\mathbb{Z}[[x]]$ different from (0) . We analyze two cases: $x \in P$ or $x \notin P$. Assume first that $x \in P$. If $P = (x)$ we are done. Otherwise,

there exists $a(x) \in P$ with $a_0 \neq 0$. Then $a_0 = a(x) - x(a_1 + a_2x + a_3x^2 + \dots) \in P$. Since P is a proper ideal, a_0 is not a unit in \mathbb{Z} and can be factorized as a product of primes, with at least one of them in P . Call this prime p . Then $(p, x) \subseteq P$. On the other hand, if $b(x) \in P$ and $b_0 \neq 0$ then, as above, $b_0 \in P$. If p does not divide b_0 , then $\gcd(b_0, p) = 1 \in P$, which is a contradiction. It follows that $p \mid b_0$ and $P = (p, x)$.

Suppose now that $x \notin P$. If $a(x)$ is a nonzero element in P , we can write $a(x) = x^m(b_0 + b_1x + b_2x^2 + \dots)$ with $b_0 \neq 0$. Since P is prime and $x \notin P$, it follows that $b_0 + b_1x + b_2x^2 + \dots \in P$. Then the image P^* of P under the natural projection $\mathbb{Z}[[x]] \rightarrow \mathbb{Z}: a(x) \mapsto a_0$ is a nonzero ideal in \mathbb{Z} , say $P^* = (q)$. Choose $q(x) \in P$ with $q_0 = q$. We first claim that q is a prime power. Using an argument by contradiction, suppose not. Then $q = st$ with s and t non-invertible and $\gcd(s, t) = 1$. Following the reasoning in Proposition 3.4, we see that $q(x) = s(x)t(x)$ with $s_0 = s$ and $t_0 = t$. One of these factors must lie in P , say $s(x)$. But then $q \mid s_0$, which is impossible by our assumption on q . Thus q must be a prime power.

We now show that $P = (q(x))$. Let $b_1(x) \in P$. Then $b_1(x) - k_1q(x) = xb_2(x) \in P$ for some $k_1 \in \mathbb{Z}$. Since $x \notin P$, we have that $b_2(x) \in P$. Similarly, there exists $k_2 \in \mathbb{Z}$ such that $b_2(x) - k_2q(x) = xb_3(x) \in P$. Continuing this argument we obtain

$$\begin{aligned} b_1(x) &= k_1q(x) + xb_2(x) = k_1q(x) + x(k_2q(x) + xb_3(x)) = \dots \\ &= q(x)(k_1 + k_2x + k_3x^2 + \dots). \end{aligned}$$

□

4 IRREDUCIBILITY CRITERIA

In this section we present some irreducibility criteria beyond the ones discussed in the previous section. We already know that if a_0 is a prime number in \mathbb{Z} , then $a(x) = \sum a_n x^n$ is irreducible in $\mathbb{Z}[[x]]$. Also, if $a_0 = pq$ with $\gcd(p, q) = 1$, then $a(x)$ is reducible. It only remains to understand the situation when $a_0 = p^\mu$ for some prime number p and a positive integer $\mu > 1$. To keep our exposition short, we will only consider the case when $a_0 = p^2$.

Suppose that $a(x) = \sum a_n x^n$ is an element of $\mathbb{Z}[[x]]$ with $a_0 = p^2$ for some prime p . If $a(x) = (\sum b_n x^n)(\sum c_n x^n)$ with $|b_0| \neq 1$ and $|c_0| \neq 1$, then $b_0 = c_0 = \pm p$ and so $a_1 = \pm p(b_1 + c_1)$. In other words,

if p does not divide a_1 , then $a(x)$ must be irreducible

Clearly, if $a(x) = p^2 + a_1x$ then $a(x)$ is irreducible if and only if $p \nmid a_1$. However, for polynomials of higher degree this condition is sufficient but not necessary. For instance, it is easy to check that $4 + 2x + 3x^2$ is irreducible.

A corresponding criterion for polynomials of the form $p^2 + a_1x + a_2x^2$ with $p \mid a_1$ and $p \nmid a_2$ does not hold. Note that, for instance, $4 - x^2$ and $4 + 4x + x^2$ can both be factored, while $4 + 4x + 3x^2$ is irreducible. However, for quadratic polynomials, we have the following criterion.

Lemma 4.1 Let $a(x) = \sum a_n x^n$ with $a_0 = p^2$ for some prime p and assume that $p \mid a_1$. If $a_2 \not\equiv \alpha\beta \pmod{p}$ for every $\alpha, \beta \in \mathbb{Z}/p\mathbb{Z}$ such that $a_1/p \equiv \alpha + \beta \pmod{p}$, then $a(x)$ is irreducible.

Proof. If $a(x) = (\sum b_n x^n)(\sum c_n x^n)$ with $|b_0| \neq 1$ and $|c_0| \neq 1$, then $a_1 = \pm p(b_1 + c_1)$. Let $\alpha \equiv \pm b_1 \pmod{p}$ and $\beta \equiv \pm c_1 \pmod{p}$. Hence $a_1/p \equiv \alpha + \beta \pmod{p}$ and $a_2 \equiv \alpha\beta \pmod{p}$. \square

The special case when $p = 2$ is particularly simple. Consider $a(x) = 4 + a_1x + a_2x^2$ with $2 \mid a_1$ and $2 \nmid a_2$. If $a_1/2 \equiv \alpha + \beta \equiv 1 \pmod{2}$, then α and β have different parity which implies that $\alpha\beta \equiv 0 \pmod{2}$. Since $\alpha\beta \equiv a_2 \not\equiv 0 \pmod{2}$, we must have that $a(x)$ is irreducible.

For an odd prime p we have the following ‘‘familiar’’ criterion. Suppose that $a_0 = p^2$ and that $a(x) = \sum a_n x^n$ is reducible. By Lemma 4.1 there exist numbers $\alpha, \beta \in \mathbb{Z}/p\mathbb{Z}$ with $a_1/p \equiv \alpha + \beta \pmod{p}$ and such that $a_2 \equiv \alpha\beta \pmod{p}$. Hence

$$(a_1/p)^2 - 4a_2 \equiv (\alpha + \beta)^2 - 4\alpha\beta \equiv (\alpha - \beta)^2 \pmod{p}$$

so that $(a_1/p)^2 - 4a_2$ is a quadratic residue \pmod{p} . In other words,

if $(a_1/p)^2 - 4a_2$ is a quadratic non-residue \pmod{p} , $a(x)$ is irreducible

According to our criteria, the polynomial $a(x) = p^2 + a_1x + a_2x^2$ with $p \mid a_1$ can be verified to be irreducible in the following situations:

p	a_1/p	a_2
3	$0 \pmod{p}$	$1 \pmod{p}$
3	$\pm 1 \pmod{p}$	$2 \pmod{p}$
5	$0 \pmod{p}$	2 or $3 \pmod{p}$
5	$\pm 1 \pmod{p}$	1 or $2 \pmod{p}$
5	$\pm 2 \pmod{p}$	3 or $4 \pmod{p}$
7	$0 \pmod{p}$	1 or 2 or $4 \pmod{p}$
7	$\pm 1 \pmod{p}$	3 or 4 or $6 \pmod{p}$
7	$\pm 2 \pmod{p}$	2 or 3 or $5 \pmod{p}$
7	$\pm 3 \pmod{p}$	1 or 5 or $6 \pmod{p}$

The following lemma gives an irreducibility criterion in $\mathbb{Z}[[x]]$ that covers, in particular, polynomials of degree 3 and 4 with $a_0 = p^2$.

Lemma 4.2 Let $a(x) = \sum a_n x^n$ with $a_0 = p^2$ for some prime p and assume that $p^2 \mid a_1$ and $p \mid a_2$. If p does not divide a_3 , then $a(x)$ is irreducible. Furthermore, if $p \mid a_3$ and if $a_4 \not\equiv \alpha\beta \pmod{p}$ for every $\alpha, \beta \in \mathbb{Z}/p\mathbb{Z}$ such that $a_2/p \equiv \alpha + \beta \pmod{p}$, then $a(x)$ is irreducible.

Proof. If $a(x) = (\sum b_n x^n)(\sum c_n x^n)$ with $|b_0| \neq 1$ and $|c_0| \neq 1$, then $b_0 = c_0 = \pm p$,

$$\begin{aligned} a_1 &= \pm p(b_1 + c_1), \\ a_2 &= \pm p(b_2 + c_2) + b_1 c_1, \\ a_3 &= \pm p(b_3 + c_3) + b_1 c_2 + b_2 c_1. \end{aligned}$$

If $p \mid a_2$, then $p \mid b_1 c_1$ so that $p \mid b_1$ or $p \mid c_1$. Further, $p^2 \mid a_1$ implies that $p \mid (b_1 + c_1)$. Thus p must divide both b_1 and c_1 , hence $p \mid a_3$. So $a(x)$ is irreducible if $p \nmid a_3$.

To prove the second statement note first that since $b_1 c_1 \equiv 0 \pmod{p^2}$, we have $a_2/p \equiv \pm(b_2 + c_2) \pmod{p}$. Let $\alpha \equiv \pm b_2 \pmod{p}$ and $\beta \equiv \pm c_2 \pmod{p}$. Since $a_4 = \pm p(b_4 + c_4) + b_1 c_3 + b_2 c_2 + b_3 c_1$, and since $b_1 \equiv c_1 \equiv 0 \pmod{p}$, we have $a_4 \equiv \alpha\beta \pmod{p}$. \square

The condition $p^2 \mid a_1$ alone cannot be relaxed to just $p \mid a_1$. Note that the cubic polynomial $p^2 + px + px^2 + x^3$ can be factorized as $(p+x)(p+x^2)$. On the other hand, the polynomial $9 + 3x + 3x^3 + x^4$ factors as $(3+x)(3+x^3)$ although the conditions on the third and fourth coefficients from Lemma 4.2 are satisfied.

The previous lemma can be generalized as follows.

Theorem 4.3 *Let $a(x) = \sum a_n x^n$ with $a_0 = p^2$ for some prime p . Assume that for some m we have $p^2 \mid a_j$ for $j = 1, \dots, m$, and $p \mid a_j$ for every even number $j \in \{m+1, \dots, 2m\}$. If p does not divide a_{2m+1} , or if $p \mid a_{2m+1}$ but $a_{2m+2} \not\equiv \alpha\beta \pmod{p}$ for every $\alpha, \beta \in \mathbb{Z}/p\mathbb{Z}$ such that $a_{m+1}/p \equiv \alpha + \beta \pmod{p}$, then $a(x)$ is irreducible.*

Proof. Assume $a(x) = (\sum b_n x^n)(\sum c_n x^n)$ with $|b_0| \neq 1$ and $|c_0| \neq 1$. Thus $b_0 = c_0 = \pm p$, and every coefficient of $a(x)$ is of the form

$$a_j = \sum_{k=0}^j b_k c_{j-k} = \pm p(b_j + c_j) + \sum_{k=1}^{j-1} b_k c_{j-k}.$$

We will prove that our assumptions on the coefficients of $a(x)$ imply

$$p \mid b_j \text{ and } p \mid c_j \text{ for } j = 1, \dots, m. \quad (1)$$

But this implies $p \mid a_{2m+1}$ since

$$a_{2m+1} = \pm p(b_{2m+1} + c_{2m+1}) + b_1 c_{2m} + \dots + b_m c_{m+1} + b_{m+1} c_m + \dots + b_{2m} c_1.$$

Thus, if $p \nmid a_{2m+1}$, then $a(x)$ is irreducible as claimed.

Moreover, if (1) holds, then

$$\sum_{k=1}^m b_k c_{m+1-k} \equiv 0 \pmod{p^2}$$

and so $a_{m+1}/p \equiv \pm(b_{m+1} + c_{m+1}) \pmod{p}$. Let $\alpha, \beta \in \mathbb{Z}/p\mathbb{Z}$ be such that $\alpha \equiv \pm b_{m+1} \pmod{p}$ and $\beta \equiv \pm c_{m+1} \pmod{p}$, so $a_{m+1}/p \equiv \alpha + \beta \pmod{p}$. Since

$$a_{2m+2} = \pm p(b_{2m+2} + c_{2m+2}) + b_1 c_{2m+1} + \cdots + b_{m+1} c_{m+1} + \cdots + b_{2m+1} c_1,$$

relation (1) implies that $a_{2m+2} \equiv \alpha\beta \pmod{p}$. Thus, if $a_{2m+2} \not\equiv \alpha\beta \pmod{p}$ for every $\alpha, \beta \in \mathbb{Z}/p\mathbb{Z}$ such that $a_{m+1}/p \equiv \alpha + \beta \pmod{p}$, then $a(x)$ must be irreducible.

We now proceed to prove (1). Assume it is false, and let $k \leq m$ be the smallest index for which $p \nmid b_k$ or $p \nmid c_k$. Thus $p \mid b_j$ and $p \mid c_j$ for $j = 1, \dots, k-1$. Since

$$a_k = \pm p(b_k + c_k) + b_1 c_{k-1} + \cdots + b_{k-1} c_1$$

and $p^2 \mid a_k$, we must have that $p \mid (b_k + c_k)$. On the other hand, since

$$a_{2k} = \pm p(b_{2k} + c_{2k}) + b_1 c_{2k-1} + \cdots + b_k c_k + \cdots + b_{2k-1} c_1$$

and $p \mid a_{2k}$, we also get $p \mid b_k c_k$. But this implies $p \mid b_k$ and $p \mid c_k$, which gives a contradiction to the assumption that (1) does not hold. \square

ACKNOWLEDGMENTS. The authors would like to thank Matt Koetz, Mark McKinzie, and Mike Weiner for helpful and cordial conversations while preparing the manuscript. They are also grateful to the referees for their valuable comments and suggestions. The first author was partially supported by a Nazareth College Summer Research grant. This article is dedicated to Susi and Ari for their love and patience.

References

- [1] J. Brewer, *Power Series Over Commutative Rings*, Lecture Notes in Pure and Applied Mathematics, vol. 64, Marcel Dekker, New York, 1981.
- [2] D. Buchsbaum, Some remarks on factorization in power series rings, *J. Math. Mech.* **10** (1961) 749–753.
- [3] D. Dummit and R. Foote, *Abstract Algebra*, Prentice-Hall, Englewood Cliffs, NJ, 1991.
- [4] D. Eisenbud, *Commutative Algebra With a View Toward Algebraic Geometry*, Graduate Texts in Mathematics, vol. 150, Springer-Verlag, New York, 1995.
- [5] I. Kaplansky, *Commutative Rings*, Allyn and Bacon, Boston, MA, 1970.
- [6] P. Samuel, On unique factorization domains, *Illinois J. Math.* **5** (1961) 1–17.
- [7] ———, Unique factorization, this MONTHLY **75** (1968) 945–952.

Daniel Birmajer graduated from the University of Buenos Aires in 1991. He worked as a high school teacher of mathematics and computer science in Argentina until 1998 when he and his family moved to the U.S. He received his Ph.D. in mathematics in 2003 from Temple University under the supervision of Professor E. S. Letzter. Since then he has been teaching at Nazareth College. He is a Sky Dot (2003) Project NExT fellow. He loves mathematics, soccer, swimming and, more than anything, his wife Susi and his children Julieta and Milton.

Department of Mathematics, Nazareth College, Rochester, NY 14618.
abirmaj6@naz.edu

Juan B. Gil was born in Venezuela where he first discovered his love for mathematics. He completed his undergraduate and graduate education in Germany and received his Ph.D. in 1998 from the University of Potsdam. In 1999 he moved to the U.S. with a visiting position at Temple University in Philadelphia. Since 2003 he has been teaching and doing research at Penn State Altoona. He is mainly interested in the analysis of PDEs and also enjoys working on problems in algebra and number theory. He is truly committed to his wife and children who asymptotically complete his life.

Penn State Altoona, 3000 Ivyside Park, Altoona, PA 16601.
jjgil@psu.edu