

FACTORIZATION OF QUADRATIC POLYNOMIALS IN THE RING OF FORMAL POWER SERIES OVER \mathbb{Z}

DANIEL BIRMAJER

*Department of Mathematics Nazareth College
4245 East Avenue, Rochester, NY 14618
abirmaj6@naz.edu*

JUAN B. GIL* and MICHAEL D. WEINER†

*Penn State Altoona
3000 Ivyside Park, Altoona, PA 16601
*jgil@psu.edu
†mdw8@psu.edu*

Received 30 July 2007

Accepted 10 October 2007

Communicated by N. Koblitz

We establish necessary and sufficient conditions for a quadratic polynomial to be irreducible in the ring $\mathbb{Z}[[x]]$ of formal power series over the integers. In particular, for polynomials of the form $p^n + p^m \beta x + \alpha x^2$ with $n, m \geq 1$ and p prime, we show that reducibility in $\mathbb{Z}[[x]]$ is equivalent to reducibility in $\mathbb{Z}_p[x]$, the ring of polynomials over the p -adic integers.

Keywords: Quadratic polynomials; power series rings; unique factorization; integral power series; p -adic numbers.

Mathematics Subject Classification 2000: 13F25, 11Y05, 13P05

1. Introduction

If K is a field, $\text{char } K \neq 2$, the question of whether or not a quadratic polynomial is reducible in the polynomial ring $K[x]$ is well understood: A polynomial $f(x) = c + bx + ax^2$, with $a \neq 0$, can be written as a product of two linear factors in $K[x]$ if and only if its discriminant $b^2 - 4ac$ is a square in K . Moreover, by Gauss' Lemma, if D is a unique factorization domain with field of fractions K , then a primitive quadratic polynomial in $D[x]$ is reducible if and only if it is reducible in $K[x]$.

If we consider the polynomials in $\mathbb{Z}[x]$ as elements of $\mathbb{Z}[[x]]$, the ring of formal power series over \mathbb{Z} , the factorization theory has a different flavor. A power series over an integral domain D is a unit in $D[[x]]$ if and only if its constant term is a unit in D , so irreducible elements in $\mathbb{Z}[x]$, such as $1 + x$, are invertible as power series.

On the other hand, any power series whose constant term is not a unit or a prime power, is reducible in $\mathbb{Z}[[x]]$, hence we can produce many examples of polynomials that are reducible as power series, yet irreducible in $\mathbb{Z}[x]$.

Similarly, when considering polynomials with integer coefficients as elements of $\mathbb{Z}[[x]]$ and as polynomials over \mathbb{Z}_p , the ring of p -adic integers, we also observe different behaviors in their arithmetic properties. For instance, the polynomial $p^2 + x + x^2$, which is irreducible as a power series, is reducible in $\mathbb{Z}_p[x]$ for any prime p . On the other hand, $6 + 2x + x^2$ is reducible in $\mathbb{Z}[[x]]$ and in $\mathbb{Z}_3[x]$, but it is irreducible in $\mathbb{Z}_2[x]$ and $\mathbb{Z}_5[x]$.

In this paper, we provide a complete picture of the factorization theory for quadratic polynomials in $\mathbb{Z}[[x]]$. In Sec. 2 we discuss the necessary background, treat some basic cases, and develop some preliminary results. In Sec. 3 we study polynomials of the form $p^n + p^m \beta x + \alpha x^2$ (the only ones not discussed in Sec. 2) and show a revealing connection between $\mathbb{Z}[[x]]$ and $\mathbb{Z}_p[x]$, cf. Theorem 3.11. In Sec. 4 we extend our results to power series and give some reducibility criteria that rely on the knowledge of their quadratic part.

A standard reference for an introduction to divisibility over integral domains is [3]. For an extensive treatment of the arithmetic on the ring of formal power series over an integral domain the reader is referred to [4] and [5]. All the necessary material about the ring \mathbb{Z}_p of p -adic numbers, can be found for instance in [2, 4, 6].

2. Factorization in the Ring of Power Series

In order to place our main result in the appropriate context, and for the reader's convenience, we review some elementary facts about the factorization theory in $\mathbb{Z}[[x]]$. First, recall that $\mathbb{Z}[[x]]$ is a unique factorization domain. Moreover, if $f(x)$ is a formal power series in $\mathbb{Z}[[x]]$ and $f_0 \in \mathbb{Z}$ is its constant term, then:

- (a) $f(x)$ is invertible if and only if $f_0 = \pm 1$.
- (b) If f_0 is prime then $f(x)$ is irreducible.
- (c) If f_0 is not a unit or a prime power then $f(x)$ is reducible.
- (d) If $f(x) = f_0$ is a constant then it is irreducible if and only if f_0 is prime.
- (e) If $f(x) = p^m + f_1 x$, with p prime and $m \geq 1$, then $f(x)$ is irreducible if and only if $\gcd(p, f_1) = 1$.

For an accessible and more detailed treatment of the divisibility theory in $\mathbb{Z}[[x]]$ the reader is referred to [1].

The above criteria are definitive for deciding irreducibility in $\mathbb{Z}[[x]]$ for constant and linear polynomials. The next natural step is to examine quadratic polynomials

$$f(x) = f_0 + f_1 x + f_2 x^2 \quad \text{with } f_2 \neq 0, f_i \in \mathbb{Z}. \quad (2.1)$$

Unless f_0 is a prime power, we know that $f(x)$ is either a unit or it is reducible in $\mathbb{Z}[[x]]$. On the other hand, if $f_0 = p^n$, $n > 1$, p prime, and if $f(x) = a(x)b(x)$ is a proper factorization, then we must have $a_0 = p^s, b_0 = p^t$ with $s, t \geq 1, s + t = n$.

This implies $f_1 = p^s b_1 + p^t a_1$, so we conclude that $f(x)$ is irreducible unless $p \mid f_1$. Therefore, for a quadratic polynomial we have:

- (f) If $f_0 = p^n$, $n > 1$, and $p \nmid f_1$, then $f(x)$ is irreducible in $\mathbb{Z}[[x]]$.
- (g) If p divides f_0 , f_1 , and f_2 , then $f(x)$ is either reducible or associate to p .

At this point, it only remains to understand polynomials of the form

$$f(x) = p^n + p^m \beta x + \alpha x^2,$$

with $n, m \geq 1$, $\gcd(p, \alpha) = 1$, and $\gcd(p, \beta) = 1$ or $\beta = 0$. We will analyze these polynomials in the next section and will produce explicit factorizations in $\mathbb{Z}[[x]]$, when appropriate. Our results will provide the following additional irreducibility criterion for the polynomial (2.1):

- (h) If $f_0 = p^n$, $n > 1$, $p \mid f_1$, and $\gcd(p, f_2) = 1$, then $f(x)$ is reducible in $\mathbb{Z}[[x]]$ if and only if it is reducible in $\mathbb{Z}_p[x]$.

Note that items (a)–(c) and (f)–(h) give complete irreducibility criteria for quadratic polynomials in $\mathbb{Z}[[x]]$.

3. Polynomials of the form $p^n + p^m \beta x + \alpha x^2$

Let p be an odd prime, let $\alpha, \beta \in \mathbb{Z}$ be such that $\gcd(p, \alpha) = 1$ and $\gcd(p, \beta) = 1$.

Proposition 3.1. *Let $f(x) = p^n + p^m \beta x + \alpha x^2$ with $n, m \geq 1$.*

- (i) *If $2m < n$, then $f(x)$ is reducible in both $\mathbb{Z}_p[x]$ and $\mathbb{Z}[[x]]$.*
- (ii) *If $2m > n$ and n is odd, then $f(x)$ is irreducible in both $\mathbb{Z}_p[x]$ and $\mathbb{Z}[[x]]$.*

Proof. (i) Observe first that the discriminant of $f(x)$ is

$$p^{2m} \beta^2 - 4\alpha p^n = p^{2m} (\beta^2 - 4\alpha p^{n-2m}),$$

a nonzero square in \mathbb{Z}_p , and so $f(x)$ is reducible in $\mathbb{Z}_p[x]$. To show that $f(x)$ is reducible as a power series, we will find sequences $\{a_k\}$ and $\{b_k\}$ such that

$$f(x) = (p^m + a_1 x + a_2 x^2 + \dots)(p^{n-m} + b_1 x + b_2 x^2 + \dots).$$

For $k \geq 1$ let $t_k = b_k + p^{n-2m} a_k$. For the above factorization to hold, we need

$$p^m \beta = p^{n-m} a_1 + p^m b_1, \text{ so we have } t_1 = \beta.$$

Let $g(x) = p^{n-2m} x^2 - \beta x + \alpha$. Since $\gcd(p, \beta) = 1$, this polynomial has a root in $\mathbb{Z}/p\mathbb{Z}$ while $g'(x) = 2p^{n-2m} x - \beta$ has none. By Hensel’s Lemma $g(x)$ has a root in $\mathbb{Z}_p[x]$ and so, in particular, there are integers a_1 and t_2 such that

$$p^{n-2m} a_1^2 - \beta a_1 + \alpha = p^m t_2.$$

Suppose that we have defined a_k, t_{k+1} for $k = 1, \dots, N - 1, N \geq 2$, and let

$$v_N = a_1 t_N + \sum_{k=2}^{N-1} a_k (t_{N+1-k} - p^{n-2m} a_{N+1-k}).$$

We want to define a_N and t_{N+1} in such a way that $\sum_{k=0}^{N+1} a_k b_{N+1-k} = 0$ for $N \geq 2$. In other words, we need

$$\begin{aligned} 0 &= \sum_{k=0}^{N+1} a_k b_{N+1-k} \\ &= a_0 b_{N+1} + a_{N+1} b_0 + a_N b_1 + a_1 b_N + \sum_{k=2}^{N-1} a_k b_{N+1-k} \\ &= p^m t_{N+1} + (\beta - p^{n-2m} a_1) a_N + a_1 (t_N - p^{n-2m} a_N) + \sum_{k=2}^{N-1} a_k b_{N+1-k} \\ &= p^m t_{N+1} + (\beta - 2p^{n-2m} a_1) a_N + v_N. \end{aligned}$$

At last, since $\gcd(p, \beta) = 1$, this equation can be solved for $t_{N+1}, a_N \in \mathbb{Z}$. This shows that $f(x)$ is reducible in $\mathbb{Z}[[x]]$.

(ii) In this case, the discriminant of $f(x)$,

$$p^{2m} \beta^2 - 4\alpha p^n = p^n (p^{2m-n} \beta^2 - 4\alpha),$$

is not a square in \mathbb{Z}_p . Thus $f(x)$ is irreducible as a polynomial over \mathbb{Z}_p . To show that $f(x)$ is irreducible as a power series, assume

$$f(x) = (p^s + a_1 x + a_2 x^2 + \dots)(p^t + b_1 x + b_2 x^2 + \dots)$$

with $t > s \geq 1, s + t = n$. Note that $t \neq s$ because n is odd. Then we must have

$$\begin{aligned} p^m \beta &= p^t a_1 + p^s b_1, \\ \alpha &= p^t a_2 + a_1 b_1 + p^s b_2. \end{aligned}$$

Since p and α are coprime, it follows that $\gcd(p, a_1) = 1 = \gcd(p, b_1)$. Therefore, it must be $s = m$, and so $2m = 2s < s + t = n$. □

It remains to analyze the cases when n is even, say $n = 2\nu$, and $m \geq \nu \geq 1$.

Proposition 3.2. *Let $m \geq \nu$. The polynomial $f(x) = p^{2\nu} + p^m \beta x + \alpha x^2$ is reducible in $\mathbb{Z}[[x]]$ if and only if $\widehat{f}(x) = p^2 + p^{m-\nu+1} \beta x + \alpha x^2$ is reducible in $\mathbb{Z}_p[x]$.*

This follows from the following three lemmas.

Lemma 3.3. *If $f(x)$ is reducible in $\mathbb{Z}[[x]]$, then $\widehat{f}(x)$ is reducible in $\mathbb{Z}[[x]]$.*

Lemma 3.4. *Let $\ell \geq 1$. If the polynomial $p^2 + p^\ell \beta x + \alpha x^2$ is reducible in $\mathbb{Z}[[x]]$, then it is reducible in $\mathbb{Z}_p[x]$.*

Lemma 3.5. *If $\widehat{f}(x)$ is reducible in $\mathbb{Z}_p[x]$, then $f(x)$ is reducible in $\mathbb{Z}[[x]]$.*

Proof of Lemma 3.3. We first observe that if $f(x) = a(x)b(x)$ is a proper factorization in $\mathbb{Z}[[x]]$, then $a_0 = b_0 = p^\nu$. To see this, assume that $a_0 = p^s$, $b_0 = p^t$ with $s, t \geq 1$, $s + t = 2\nu$. Then we have that

$$\alpha = p^s b_2 + a_1 b_1 + p^t a_2.$$

Since $\gcd(p, \alpha) = 1$, we conclude that $\gcd(p, a_1) = \gcd(p, b_1) = 1$. We also have

$$p^m \beta = p^s b_1 + p^t a_1.$$

If $s < t$, then we would have $s < \nu \leq m$, implying from the above equation that $p \mid b_1$, a contradiction. Similarly, we can rule out the case $t < s$, hence $s = t = \nu$.

We now write $f(x) = a(x)b(x)$ with $a_0 = b_0 = p^\nu$. Since

$$p^{2\nu-2} \widehat{f}(x) = f(p^{\nu-1}x) = a(p^{\nu-1}x)b(p^{\nu-1}x),$$

it follows that

$$\widehat{f}(x) = \left(\frac{a(p^{\nu-1}x)}{p^{\nu-1}} \right) \left(\frac{b(p^{\nu-1}x)}{p^{\nu-1}} \right)$$

is a proper factorization of $\widehat{f}(x)$ in $\mathbb{Z}[[x]]$. □

Proof of Lemma 3.4. To prove that $g(x) = p^2 + p^\ell \beta x + \alpha x^2$ is reducible in $\mathbb{Z}_p[x]$, we must show that its discriminant $p^{2\ell} \beta^2 - 4\alpha p^2$ is a square in \mathbb{Z}_p .

If the discriminant is zero, we are done. Otherwise, write $p^{2\ell-2} \beta^2 - 4\alpha = p^t u$ with $\gcd(p, u) = 1$. Suppose that $g(x)$ is reducible in $\mathbb{Z}[[x]]$. Without loss of generality we can assume that $g(x)$ admits a factorization of the form

$$p^2 + p^\ell \beta x + \alpha x^2 = a(x)b(x) \quad \text{with } a_0 = b_0 = p, \quad a_2 = a_3 = \cdots = a_{t+2} = 0.$$

With the notation $s_j = a_j + b_j$ for $j \geq 1$, we must have

$$\begin{aligned} p^\ell \beta &= p s_1, \\ \alpha &= p s_2 + a_1 s_1 - a_1^2. \end{aligned}$$

Then $s_1 = p^{\ell-1} \beta$ and a_1 is a root of $y^2 - s_1 y + \alpha \equiv 0 \pmod{p}$. Note that $p \nmid a_1$.

For $n = 3$ we have

$$0 = p s_3 + a_1 s_2. \tag{3.6}$$

Then $p \mid s_2$ and $a_1^2 - a_1 s_1 + \alpha \equiv 0 \pmod{p^2}$. For $n = 4$ we have

$$0 = p s_4 + a_1 s_3.$$

Then $p \mid s_3$, which by (3.6) implies that $p^2 \mid s_2$, and so $a_1^2 - a_1 s_1 + \alpha \equiv 0 \pmod{p^3}$.

Working inductively, the equation

$$0 = p s_{t+3} + a_1 s_{t+2}$$

implies that $p^{t+1} \mid s_2$, and so $a_1^2 - a_1 s_1 + \alpha = p^{t+2} v$ for some v .

Now, since

$$(2a_1 - s_1)^2 = (p^{2\ell-2}\beta^2 - 4\alpha) + 4p^{t+2}v = p^t u + 4p^{t+2}v = p^t(u + 4p^2v),$$

and since $\gcd(p, u) = 1$, we have that t is even and that u is a square mod p . Hence $p^{2(\ell-1)}\beta^2 - 4\alpha$ is a square in \mathbb{Z}_p , and so is $p^2(p^{2(\ell-1)}\beta^2 - 4\alpha)$. Therefore, $g(x)$ is reducible in $\mathbb{Z}_p[x]$. □

Proof of Lemma 3.5. We will consider the cases $m = \nu$ and $m > \nu$ separately. In both cases we will prove the reducibility of $f(x)$ in $\mathbb{Z}[[x]]$ by providing an explicit factorization algorithm. More precisely, we will give inductive algorithms (depending on m and ν) to find sequences $\{a_k\}$ and $\{b_k\}$ in \mathbb{Z} such that

$$f(x) = \left(\sum_{k=0}^{\infty} a_k x^k \right) \left(\sum_{k=0}^{\infty} b_k x^k \right). \tag{3.7}$$

For $k \geq 1$ we let $s_k = a_k + b_k$.

Case 1. Let $m > \nu$. Since $\widehat{f}(x) = p^2 + p^{m-\nu+1}\beta x + \alpha x^2$ is reducible in $\mathbb{Z}_p[x]$, the polynomial $\widehat{g}(x) = x^2 - p^{m-\nu}\beta x + \alpha$ is reducible in $\mathbb{Z}_p[x]$, too. Observe that the discriminant of $\widehat{f}(x)$ is p^2 times the discriminant of $\widehat{g}(x)$.

Let

$$a_0 = p^\nu = b_0 \quad \text{and} \quad s_1 = p^{m-\nu}\beta.$$

Since $\widehat{g}(x)$ is reducible in $\mathbb{Z}_p[x]$, it has a root in $\mathbb{Z}/p^\nu\mathbb{Z}$. Let $a_1, s_2 \in \mathbb{Z}$ be such that

$$a_1^2 - p^{m-\nu}\beta a_1 + \alpha = p^\nu s_2.$$

Now, $m > \nu$ and $\gcd(p, \alpha) = 1$ imply $\gcd(p, a_1) = 1$ and $\gcd(p^\nu, p^{m-\nu}\beta - 2a_1) = 1$. We let a_2 and s_3 be integer numbers such that

$$0 = p^\nu s_3 + (p^{m-\nu}\beta - 2a_1)a_2 + a_1 s_2.$$

Suppose we have defined a_k and s_{k+1} for $k = 1, \dots, N - 1$, $N \geq 3$, and let

$$v_N = a_1 s_N + \sum_{k=2}^{N-1} a_k (s_{N+1-k} - a_{N+1-k}).$$

We know that $\gcd(p^\nu, p^{m-\nu}\beta - 2a_1) = 1$, so the equation

$$0 = p^\nu s_{N+1} + (p^{m-\nu}\beta - 2a_1)a_N + v_N$$

can be solved for $a_N, s_{N+1} \in \mathbb{Z}$. For $k = 1, \dots, N$ we now have a_k and b_k , and it can be easily checked that the sequences $\{a_k\}$ and $\{b_k\}$ give (3.7).

Case 2. If $m = \nu$, then

$$\widehat{f}(x) = p^2 + p\beta x + \alpha x^2 \quad \text{and} \quad f(x) = p^{2\nu} + p^\nu \beta x + \alpha x^2.$$

Since $\widehat{f}(x)$ is reducible in $\mathbb{Z}_p[x]$, so is $\widehat{g}(x) = x^2 - \beta x + \alpha$. If $\beta^2 - 4\alpha = 0$, then β is even and $f(x) = (\frac{\beta}{2}x + p^\nu)^2$, which is a proper factorization in $\mathbb{Z}[[x]]$. If $\beta^2 - 4\alpha \neq 0$, there are numbers $\ell \in \mathbb{N}_0$ and $q \in \mathbb{Z}$ such that

$$\beta^2 - 4\alpha = p^{2\ell} q \quad \text{with} \quad \gcd(p, q) = 1.$$

Moreover, $\widehat{g}(x)$ has a root in $\mathbb{Z}/p^n\mathbb{Z}$ for every $n \in \mathbb{N}$. In particular, for $n = 3 \max(\ell, \nu)$, there are integers a and r such that

$$a^2 - \beta a + \alpha = p^\mu r \quad \text{with} \quad \gcd(p, r) = 1, \tag{3.8}$$

for some $\mu \geq 3 \max(\ell, \nu)$. Since $(\beta - 2a)^2 - (\beta^2 - 4\alpha) = 4\widehat{g}(a)$, we get

$$(\beta - 2a)^2 = 4p^\mu r + p^{2\ell} q = p^{2\ell} (4p^{\mu-2\ell} r + q),$$

hence we can write

$$\beta - 2a = p^\ell t \quad \text{with} \quad \gcd(p, t) = 1. \tag{3.9}$$

Again, our goal is to construct sequences $\{a_k\}$ and $\{b_k\}$ such that (3.7) holds. This will be done with slightly different algorithms for $\nu > \ell$ and $\nu \leq \ell$. In both cases we let

$$\begin{aligned} a_0 &= p^\nu = b_0, & s_1 &= \beta, \\ a_1 &= a, & s_2 &= p^{\mu-\nu} r, \end{aligned}$$

where a and r are the integers from (3.8). With these choices, the first three terms in the expansion of (3.7) coincide with $f(x)$.

Assume $\nu > \ell$. Let

$$\tilde{a}_1 = 0, \quad u_1 = s_2 = p^{\mu-\nu} r, \quad \text{and} \quad u_2 = -p^{\mu-2\nu} r a_1.$$

Let t be as in (3.9). For $k \geq 2$ we will define \tilde{a}_k and u_{k+1} such that the sequences defined by

$$a_k = p^{\nu-\ell} \tilde{a}_k \quad \text{and} \quad b_k = u_{k-1} - t \tilde{a}_{k-1} - a_k \tag{3.10}$$

give the factorization (3.7). Note that $s_{k+1} = a_{k+1} + b_{k+1} = u_k - t \tilde{a}_k$.

Let $\tilde{a}_2 = p^{\mu-2\nu}$ and $u_3 = -p^{\mu-3\nu} [p^{\nu-\ell}(s_2 - a_2) - t a_1]$. Thus

$$p^\nu u_3 + [p^{\nu-\ell}(s_2 - a_2) - t a_1] \tilde{a}_2 = 0.$$

Suppose we have defined \tilde{a}_k and u_{k+1} for $k = 1, \dots, N - 1$, $N \geq 3$, and let

$$v_N = a_1 u_N + a_2 s_N + \sum_{k=3}^{N-1} a_k (s_{N+2-k} - a_{N+2-k}).$$

Since $\gcd(p, \beta) = 1$, the relation (3.9) implies

$$\gcd(p, a_1) = 1 \quad \text{and} \quad \gcd(p^{\nu-\ell}, p^{\nu-\ell}(s_2 - 2a_2) - t a_1) = 1.$$

Therefore, there are $\tilde{a}_N, u_{N+1} \in \mathbb{Z}$ such that

$$p^\nu u_{N+1} + [p^{\nu-\ell}(s_2 - 2a_2) - ta_1]\tilde{a}_N + v_N = 0.$$

The sequences $\{a_k\}$ and $\{b_k\}$ defined by (3.10) give (3.7) when $\nu > \ell$.

Assume now $\nu \leq \ell$. In this case, for $k \geq 2$ we will find \tilde{a}_k and \tilde{s}_{k+1} such that the sequences defined by

$$a_k = p^\ell \tilde{a}_k \quad \text{and} \quad b_k = p^{3\ell-\nu} \tilde{s}_k - a_k$$

give a factorization of $f(x)$. Let r and t be as in (3.8) and (3.9), respectively. Since $\gcd(p^\nu, t) = 1$, there are $y, z \in \mathbb{Z}$ such that

$$p^\nu y + tz + r = 0.$$

Let $\tilde{a}_2 = p^{\mu-2\ell-\nu} z a_1$, $\tilde{s}_2 = p^{\mu-3\ell} r$, and $\tilde{s}_3 = p^{\mu-3\ell} y a_1$. Note that

$$p^\ell \tilde{s}_3 + t\tilde{a}_2 + a_1 p^{\ell-\nu} \tilde{s}_2 = 0.$$

Suppose we have defined \tilde{a}_k and \tilde{s}_{k+1} for $k = 1, \dots, N - 1$, $N \geq 3$, and let

$$\tilde{v}_N = a_1 p^{\ell-\nu} \tilde{s}_N + \sum_{k=2}^{N-1} \tilde{a}_k (p^{2\ell-\nu} \tilde{s}_{N+1-k} - \tilde{a}_{N+1-k}).$$

Finally, since $\gcd(p^\ell, t) = 1$, the equation

$$0 = p^\ell \tilde{s}_{N+1} + t\tilde{a}_N + \tilde{v}_N$$

can be solved for $\tilde{a}_N, \tilde{s}_{N+1} \in \mathbb{Z}$. This implies

$$\begin{aligned} 0 &= p^{3\ell} \tilde{s}_{N+1} + p^{2\ell} t \tilde{a}_N + p^{2\ell} \tilde{v}_N \\ &= p^\nu s_{N+1} + p^\ell t a_N + a_1 s_N + \sum_{k=2}^{N-1} a_k (s_{N+1-k} - a_{N+1-k}) \\ &= p^\nu s_{N+1} + (\beta - 2a_1) a_N + a_1 s_N + \sum_{k=2}^{N-1} a_k b_{N+1-k} = \sum_{k=0}^{N+1} a_k b_{N+1-k}, \end{aligned}$$

as desired. This completes the proof. □

The main result of this section is the following.

Theorem 3.11. *Let p be an odd prime and let $n, m \geq 1$. Let $\alpha, \beta \in \mathbb{Z}$ be such that $\gcd(p, \alpha) = 1$ and $\gcd(p, \beta) = 1$. The polynomial $f(x) = p^n + p^m \beta x + \alpha x^2$ is reducible in $\mathbb{Z}[[x]]$ if and only if it is reducible in $\mathbb{Z}_p[x]$.*

Proof. Using the fact that $f(x)$ is reducible in $\mathbb{Z}_p[x]$ iff $\widehat{f}(x)$ is reducible in $\mathbb{Z}_p[x]$, the statement of the theorem follows from Proposition 3.1 and Proposition 3.2. □

Remark 3.12. The previous theorem is not valid when $m = 0$. In fact, if $p \nmid \beta$, any power series of the form $p^n + \beta x + \dots$ is irreducible in $\mathbb{Z}[[x]]$. However, any polynomial $p^n + \beta x + \alpha x^2$ with $\gcd(p, \beta) = 1$ is reducible in $\mathbb{Z}_p[x]$.

We finish this section with the remaining case: $\beta = 0$.

Proposition 3.13. *Let p be an odd prime and let $n \geq 1$. Let $\alpha \in \mathbb{Z}$ be such that $\gcd(p, \alpha) = 1$. The polynomial $f(x) = p^n + \alpha x^2$ is reducible in $\mathbb{Z}[[x]]$ if and only if it is reducible in $\mathbb{Z}_p[x]$.*

Proof. Recall that $f(x) = p^n + \alpha x^2$ is reducible in $\mathbb{Z}_p[x]$ if and only if its discriminant $-4\alpha p^n$ is a nonzero square in \mathbb{Z}_p . This in turn is the case if and only if n is even and $-\alpha$ is a square in $\mathbb{Z}/p\mathbb{Z}$. We will show that these conditions on n and α are equivalent to $f(x)$ being reducible in $\mathbb{Z}[[x]]$.

For $f(x)$ to admit a factorization of the form

$$p^n + \alpha x^2 = (a_0 + a_1x + a_2x^2 + \dots)(b_0 + b_1x + b_2x^2 + \dots)$$

it is necessary to solve the equations

$$\begin{aligned} a_0 = p^t \quad \text{and} \quad b_0 = p^s \quad & \text{with } t + s = n, \\ 0 = p^t b_1 + p^s a_1, \\ \alpha = p^t b_2 + a_1 b_1 + p^s a_2. \end{aligned}$$

Since $\gcd(p, \alpha) = 1$, these three equations can be solved in \mathbb{Z} only when $s = t$, that is, when n is even. Now, if $n = 2\nu$, we must have $a_0 = b_0 = p^\nu$, $s_1 = a_1 + b_1 = 0$, and $\alpha = p^\nu(a_2 + b_2) - a_1^2$. Thus, if $f(x)$ is reducible in $\mathbb{Z}[[x]]$, then $-\alpha$ is a square in $\mathbb{Z}/p\mathbb{Z}$. On the other hand, if $-4\alpha p^{2\nu}$ is a nonzero square in \mathbb{Z}_p , so is $-\alpha$, i.e. $y^2 + \alpha$ has a root in \mathbb{Z}_p . Let a_1 and s_2 be integers such that

$$a_1^2 + \alpha = p^\nu s_2.$$

Note that $\gcd(p^\nu, 2a_1) = 1$. Therefore, there are integers a_2 and s_3 such that

$$0 = p^\nu s_3 - 2a_1 a_2 + a_1 s_2.$$

Finally, a factorization of $f(x)$ in $\mathbb{Z}[[x]]$ can be obtained with the sequences $\{a_k\}$ and $\{s_{k+1}\}$ defined inductively for $N \geq 3$ by the equation

$$0 = p^\nu s_{N+1} - 2a_1 a_N + v_N,$$

where $v_N = a_1 s_N + \sum_{k=2}^{N-1} a_k (s_{N+1-k} - a_{N+1-k})$. □

Remark 3.14. With the appropriate adjustments in the proofs, all the results in this section apply verbatim to the case when $p = 2$. For the interested reader, we recall that an element $2^n u \in \mathbb{Q}_2^*$ is a square iff n is even and $u \equiv 1 \pmod{8}$.

4. Further Reducibility Criteria

In this last section we briefly discuss the factorization in $\mathbb{Z}[[x]]$ of power series whose quadratic part is a polynomial like the ones studied in the previous sections. More precisely, we consider power series of the form

$$f(x) = p^n + p^m \beta x + \alpha x^2 + \sum_{k=3}^{\infty} c_k x^k, \tag{4.1}$$

where α and β are integers such that $\gcd(p, \alpha) = 1 = \gcd(p, \beta)$.

For simplicity, we only discuss the case when p is an odd prime. We will focus on the situations for which the arguments in Sec. 3 extend with little or no additional effort. For instance, if $m \neq \frac{n}{2}$, the reducibility of $f(x)$ in $\mathbb{Z}[[x]]$ follows the same pattern as the reducibility of its quadratic part. In fact, we can use the exact same arguments from Sec. 3 to prove the following two propositions.

Proposition 4.2. *If $2m < n$, then (4.1) is reducible in $\mathbb{Z}[[x]]$. If $2m > n$ and n is odd, then (4.1) is irreducible.*

Proposition 4.3. *If $2m > n$ and n is even, then (4.1) is reducible in $\mathbb{Z}[[x]]$ if and only if $-\alpha$ is a quadratic residue mod p .*

If $2m = n$, the situation is in general more involved and the reducibility of $f(x)$ depends on the roots of $x^2 - \beta x + \alpha$. The following proposition is easy to prove.

Proposition 4.4. *If $2m = n$ and the polynomial $x^2 - \beta x + \alpha$ has a simple root in $\mathbb{Z}/p^m\mathbb{Z}$, then (4.1) is reducible in $\mathbb{Z}[[x]]$.*

If $x^2 - \beta x + \alpha$ has a double root in $\mathbb{Z}/p^m\mathbb{Z}$, it is not enough to look at the quadratic part of $f(x)$ and its reducibility depends on the coefficients c_k . To illustrate this fact, consider for example the power series

$$f(x) = p^2 + p\beta x + \alpha x^2 + c_3 x^3 + c_4 x^4 + \dots,$$

with $\alpha, \beta \in \mathbb{Z}$ such that $\beta^2 - 4\alpha = p^2 q$, where q is a quadratic residue mod p with $\gcd(p, q) = 1$. In order to get a proper factorization $f(x) = a(x)b(x)$ in $\mathbb{Z}[[x]]$, we must have $a_0 = p = b_0$, $\beta = s_1$, as well as

$$\begin{aligned} \alpha &= ps_2 + a_1(\beta - a_1), \\ c_3 &= ps_3 + (\beta - 2a_1)a_2 + a_1s_2, \end{aligned}$$

where $s_k = a_k + b_k$. Then $(\beta - 2a_1)^2 - (\beta^2 - 4\alpha) = 4ps_2$, which implies $p \mid s_2$. Therefore, $f(x)$ is irreducible in $\mathbb{Z}[[x]]$ unless $p \mid c_3$.

On the other hand, if $p^2 \mid c_k$ for every $k \geq 3$, then with the same assumptions on α and β as above, we can find $a_k, b_k \in \mathbb{Z}$ such that $a(x) = \sum a_k x^k$ and $b(x) = \sum b_k x^k$ give a proper factorization $f(x) = a(x)b(x)$. Note that $\beta^2 - 4\alpha$ is a square in \mathbb{Z}_p , so the polynomial $g(x) = x^2 - \beta x + \alpha$ is reducible in $\mathbb{Z}_p[x]$. In particular, $g(x)$ has a root in $\mathbb{Z}/p^3\mathbb{Z}$, so there are $a, r \in \mathbb{Z}$ such that

$$a^2 - \beta a + \alpha = p^3 r.$$

Moreover, since $(\beta - 2a)^2 - (\beta^2 - 4\alpha) = 4p^3 r$ and $p^2 \mid (\beta^2 - 4\alpha)$, we have $p \mid (\beta - 2a)$. In fact, there is an integer t with $\gcd(p, t) = 1$ such that

$$\beta - 2a = pt.$$

Choose $a_1 = a$, $\tilde{s}_2 = r$, and write $c_{k+1} = p^2 \tilde{c}_{k+1}$. Since $\gcd(p, t) = 1$, for $k \geq 2$ we can choose \tilde{a}_k and \tilde{s}_{k+1} inductively as integer solutions of the equation

$$\tilde{c}_{k+1} = p\tilde{s}_{k+1} + t\tilde{a}_k + a_1\tilde{s}_k + \sum_{j=2}^{k-1} \tilde{a}_j (p\tilde{s}_{k+1-j} - \tilde{a}_{k+1-j}).$$

If we let $a_k = p\tilde{a}_k$ and $s_k = p^2\tilde{s}_k$, then multiplication by p^2 gives

$$\begin{aligned} c_{k+1} &= ps_{k+1} + pta_k + a_1s_k + \sum_{j=2}^{k-1} a_j(s_{k+1-j} - a_{k+1-j}) \\ &= ps_{k+1} + (\beta - 2a_1)a_k + a_1s_k + \sum_{j=2}^{k-1} a_jb_{k+1-j} \\ &= \sum_{j=0}^{k+1} a_jb_{k+1-j}. \end{aligned}$$

In other words, $a(x)$ and $b(x)$ provide a factorization of $f(x)$ in $\mathbb{Z}[[x]]$, as claimed.

References

- [1] D. Birmajer and J. B. Gil, Arithmetic in the ring of formal power series with integer coefficients, to appear in *American Mathematical Monthly*.
- [2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, trans. from Russian by N. Greenleaf (Academic Press, New York, 1966).
- [3] D. Dummit and R. Foote, *Abstract Algebra* (Prentice-Hall, 1991).
- [4] D. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, Graduate Texts in Mathematics (Springer, 1995).
- [5] I. Kaplansky, *Commutative Rings* (Allyn and Bacon, Inc., Boston, 1970).
- [6] J.-P. Serre, *A Course in Arithmetic*, Graduate Texts in Mathematics (Springer, 1973).