Comm. Algebra 39(4) 2011, pp 1482–1490

Non-unique factorization of polynomials over residue class rings of the integers

Christopher Frei and Sophie Frisch

Abstract. We investigate non-unique factorization of polynomials in $\mathbb{Z}_{p^n}[x]$ into irreducibles. As a Noetherian ring whose zero-divisors are contained in the Jacobson radical, $\mathbb{Z}_{p^n}[x]$ is atomic. We reduce the question of factoring arbitrary non-zero polynomials into irreducibles to the problem of factoring monic polynomials into monic irreducibles. The multiplicative monoid of monic polynomials of $\mathbb{Z}_{p^n}[x]$ is a direct sum of monoids corresponding to irreducible polynomials in $\mathbb{Z}_p[x]$, and we show that each of these monoids has infinite elasticity. Moreover, for every $m \in \mathbb{N}$, there exists in each of these monoids a product of 2 irreducibles that can also be represented as a product of m irreducibles.

Keywords: polynomial, finite ring, non-unique factorization, elasticity, zero-divisor, monoid. MSC 2000: Primary 13M10; Secondary 13P05, 11T06, 20M14.

1. Introduction

Polynomials with coefficients in $\mathbb{Z}_{p^n} = \mathbb{Z}/p^n\mathbb{Z}$, p prime, $n \geq 2$, have been investigated quite a lot with respect to the polynomial functions they define [6, 9, 4]. Comparatively little is known about the multiplicative monoid of non-zerodivisors of $\mathbb{Z}_{p^n}[x]$. McDonald [7] and Wan [8] list a few properties concerning uniqueness of certain kinds of factorizations of polynomials in $\mathbb{Z}_{p^n}[x]$. At the same time, factorization into irreducibles is manifestly non-unique. In this paper, we investigate non-uniqueness of factorization of polynomials in $\mathbb{Z}_{p^n}[x]$ into irreducibles, in the spirit of [5]. Throughout this paper, p is a fixed prime and $n \geq 2$.

Here is an example of the phenomena we will study. Consider the identity in $\mathbb{Z}_{p^n}[x]$:

$$(x^m + p^{n-1})(x^m + p) = x^m(x^m + p^{n-1} + p).$$

Assuming for the moment that every element of $\mathbb{Z}_{p^n}[x]$ has a factorization into irreducible elements (cf. Corollary 2.9), we note that $(x^m + p^{n-1})$ is a product of at most $n-1$ irreducibles, and that $(x^m + p)$ is irreducible. This is so because both polynomials represent a power of x in $\mathbb{Z}_p[x]$. By unique factorization in $\mathbb{Z}_p[x]$, each of their factors in $\mathbb{Z}_{p^n}[x]$ (apart from units) also represents a power of x in $\mathbb{Z}_p[x]$. (We have used the fact that a polynomial in $\mathbb{Z}_{p^n}[x]$ is a unit if and only if it maps to a unit in $\mathbb{Z}_p[x]$ under canonical projection.) Since every non-unit factor in $\mathbb{Z}_{p^n}[x]$ of $(x^m + p^{n-1})$ or $(x^m + p)$ represents a power of x in $\mathbb{Z}_p[x]$, the constant coefficient of every such factor is divisible by p. On the other hand, the constant coefficient of $(x^m + p^{n-1})$ is divisible by no higher power of p than p^{n-1}, so it cannot be a product of more than $n-1$ non-unit polynomials, and $(x^m + p)$ cannot be a product of more than one non-unit in $\mathbb{Z}_{p^n}[x]$. We have seen that for arbitrary $m \in \mathbb{N}$, there exists in $\mathbb{Z}_{p^n}[x]$ a product of at most n irreducibles that is also representable as a product of more than m irreducibles.

We now establish some notation:

1.1. Definition. We denote p-adic valuation on $\mathbb{Q}$ by v and extend v to $\mathbb{Q}(x)$ by defining $v(f) = \min_k v(a_k)$ for $f = \sum_k a_k x^k \in \mathbb{Z}[x]$, and $v(f/g) = v(f) - v(g)$. This gives a surjective mapping $v\colon \mathbb{Z}[x] \to \mathbb{N}_0 \cup \{\infty\}$.

We denote by $(N_n, +, \leq)$ the ordered monoid with elements $0, 1, \ldots, n-1, \infty$ resulting from factoring $(\mathbb{N}_0 \cup \{\infty\}, +, \leq)$ by the congruence relation that identifies all values greater or equal n, including ∞. By abuse of notation, we still use v for the surjective mapping $v\colon \mathbb{Z}_{p^n}[x] \to N_n$ obtained by factoring p-adic valuation $v\colon \mathbb{Z}[x] \to \mathbb{N}_0 \cup \{\infty\}$ by the above congruence relation.

The mapping $v\colon \mathbb{Z}_{p^n}[x] \to N_n$ behaves like a valuation, except that $(N_n, +, \leq)$ is not a group (nor can it be extended to a group, as it is not cancellative).

1.2. Remark. *$v\colon \mathbb{Z}_{p^n}[x] \to N_n$ satisfies*

(i) $v(f) = \infty \iff f = 0$

(ii) $v(f+g) \geq \min(v(f), v(g))$

(iii) $v(f \cdot g) = v(f) + v(g)$

We will write p for a prime in $\mathbb{Z}$ as well as for its residue class in $\mathbb{Z}_{p^n}$ or $\mathbb{Z}_{p^n}[x]$. This should not cause any confusion; we are always going to specify which ring we are talking about. In the remainder of this section, we review a few well-known facts about $\mathbb{Z}_{p^n}[x]$.

1.3. Fact. *For $f \in \mathbb{Z}_{p^n}[x]$, the following are equivalent:*

(a) *$v(f) > 0$, i.e., all coefficients of f are divisible (in $\mathbb{Z}_{p^n}$) by p.*

(b) *f is nilpotent.*

(c) *f is a zero-divisor.*

Proof. This follows from the properties of $v\colon \mathbb{Z}_{p^n}[x] \to N_n$ mentioned in 1.2. $\square$

1.4. Definition. Let R be a commutative ring.

(i) $\mathrm{Nil}(R)$ denotes the nilradical of R, i.e., the intersection of all prime ideals of R.

(ii) $\mathrm{J}(R)$ denotes the Jacobson radical of R, i.e., the intersection of all maximal ideals of R.

(iii) $\mathrm{Z}(R)$ denotes the set of zero-divisors of R.

(iv) $\mathrm{U}(R)$ denotes the group of units of R.

As we all know, the intersection of all prime ideals of a commutative ring coincides with the set of nilpotent elements:

$$\mathrm{Nil}(R) \quad = \bigcap_{P \text{ prime}} P \quad = \quad \{r \in R \mid \exists n \in \mathbb{N} \;\; r^n = 0\}.$$

1.5. Fact.

$$\mathrm{Nil}(\mathbb{Z}_{p^n}[x]) = \mathrm{J}(\mathbb{Z}_{p^n}[x]) = (p) = \mathrm{Z}(\mathbb{Z}_{p^n}[x])$$

Proof. Since the maximal ideals of $\mathbb{Z}_{p^n}[x]$ are precisely the ideals (p, f) with f representing an irreducible polynomial in $\mathbb{Z}_p[x]$, we see $\mathrm{J}(\mathbb{Z}_{p^n}[x]) = (p)$. We already know $(p) = \mathrm{Nil}(\mathbb{Z}_{p^n}[x]) = \mathrm{Z}(\mathbb{Z}_{p^n}[x])$ from Fact 1.3. $\square$

1.6. Fact. *Let R be a commutative ring. The units of $R[x]$ are precisely the polynomials $a_0 + a_1x + \ldots + a_nx^n$ with a_0 a unit of R and a_k nilpotent for $k > 0$.*

Proof. If f is a unit then its image under projection to $(R/P)[x]$ is a unit for every prime ideal P of R. Therefore, a_0 is not in any P and hence a unit; and for $k > 0$, a_k is in every P and therefore nilpotent. Conversely, if $f = a_0 + g$ with a_0 a unit of R and all coefficients of g in the intersection of all prime ideals of R, then g is in every prime ideal of $R[x]$ and hence $f = a_0 + g$ is in no prime ideal of $R[x]$ and therefore a unit of $R[x]$. $\square$

1.7. Corollary. *Let p be a prime and $n \geq 1$. Then $\mathrm{U}(\mathbb{Z}_{p^n}[x])$ consists of precisely the polynomials $f = a_0 + a_1x + \ldots + a_nx^n$ such that (in $\mathbb{Z}_{p^n}$) $p \nmid a_0$ and $p \mid a_k$ for $k > 0$. It follows that a polynomial in $\mathbb{Z}[x]$ represents a unit in $\mathbb{Z}_{p^n}[x]$ for some $n \geq 1$ if and only if it represents a unit in $\mathbb{Z}_{p^n}[x]$ for all n.*

2. Different concepts of irreducibility in rings with zero-divisors

Various facts about irreducible and prime elements that are clear in integral domains tend to become messy and obfuscated as soon as zero-divisors are involved. We will see, however, that everything works just as smoothly as in integral domains if all zero-divisors are contained in the Jacobson radical. For an in-depth investigation of factorization in rings with zero-divisors see [2, 3, 1]. The very natural concepts defined in this section appear in the literature ([2, 3, 1] and their references) under varying names. Our choice of names has been motivated by a desire to define *associated* and *irreducible* for commutative rings just like they are usually defined for integral domains and to reflect the existence of a group of "stronger" concepts (associated, irreducible, atomic), and a parallel group of "weaker" concepts, with analogous relationships between the concepts inside each group. R is always a commutative ring with identity.

2.1. Definition. If $c \in R$ is a non-zero non-unit then we say that c is *weakly irreducible* if for all $a, b \in R$

$$c = ab \Longrightarrow c \mid a \text{ or } c \mid b$$

and that c is *irreducible* if for all $a, b \in R$

$$c = ab \Longrightarrow b \text{ is a unit or } a \text{ is a unit.}$$

A non-zero non-unit c is called *prime* if for all $a, b \in R$

$$c \mid ab \Longrightarrow c \mid a \text{ or } c \mid b$$

2.2. Definition. Let $a, b \in R$. We call a and b *weakly associated* if $a \mid b$ and $b \mid a$ (or equivalently, if $(a) = (b)$). We call a and b *associated* if there exists a unit $u \in R$ such that $a = bu$.

It is clear that irreducible implies weakly irreducible, that associated implies weakly associated, and that both converses hold in integral domains. Also, prime implies irreducible in integral domains. We now consider a class of commutative rings properly containing the class of integral domains in which the implications mentioned above still hold.

2.3. Definition. Let R be a commutative ring. We say that R is a ring with *harmless zero-divisors*, if $\mathrm{Z}(R) \subseteq 1 - \mathrm{U}(R) = \{1 - u \mid u \text{ a unit of } R\}$. (These are the rings called *présimplifiable* by Bouvier (cf. [2]).)

2.4. Lemma. ([2]). *Let R be a ring with harmless zero-divisors and $a, b, c, u, v \in R$. Then*

(1) *if $a \neq 0$, $a = bu$ and $b = av$ then u, v are units;*
(2) *a, b are weakly associated if and only if they are associated;*
(3) *c is weakly irreducible if and only if c is irreducible;*
(4) *if c is prime then c is irreducible.*

Proof. (1) $a = avu$; therefore $a(1 - vu) = 0$, which makes $(1 - vu)$ a zero-divisor. Now $1 - vu = 1 - w$ for some unit w; hence $vu = w$ and u, v are units. (2), (3) and (4) follow from (1). $\square$

2.5. Corollary. If a commutative ring R satisfies $\mathrm{Z}(R) \subseteq \mathrm{J}(R)$ then the statements of Lemma 2.4 hold for R. In particular, they hold for $\mathbb{Z}_{p^n}[x]$.

Proof. It is easy to see that $\mathrm{J}(R) \subseteq 1 - \mathrm{U}(R)$ holds in every commutative ring. Therefore every ring satisfying $\mathrm{Z}(R) \subseteq \mathrm{J}(R)$ is a ring with harmless zero-divisors. In particular, $\mathbb{Z}_{p^n}[x]$ is a ring with harmless zero-divisors, since $\mathrm{Z}(\mathbb{Z}_{p^n}[x]) = \mathrm{J}(\mathbb{Z}_{p^n}[x])$ by Fact 1.5. $\square$

2.6. Definition. Let R be a commutative ring. R is called *atomic* if every non-zero non-unit is a product of irreducible elements. We call R *weakly atomic* if every non-zero non-unit is a product of weakly irreducible elements.

If one examines the usual proof that an integral domain with ACC for principal ideals is atomic, one finds that it shows that any commutative ring with ACC for principal ideals is weakly atomic. Namely, suppose there exists an element s in the set S of those non-zero non-units of R that do not factor into weakly irreducible elements. Then s is not weakly irreducible, so there exist a, b with $s = ab$ and $s \nmid a$, $s \nmid b$. Such a, b must be non-zero non-units, and at least one of them is in S; say $a \in S$. As $a \mid s$ and $s \nmid a$, we have $(s) \subset (a)$. By iteration we get an infinite ascending chain of principal ideals. We have shown:

2.7. Lemma. ([2] Thm. 3.2). *If R is a commutative ring satisfying ACC for principal ideals then R is weakly atomic.*

Combining Lemmas 2.4 and 2.7, we obtain

2.8. Lemma. ([2]). *Every commutative ring with harmless zero-divisors satisfying ACC for principal ideals is atomic; in particular, every Noetherian ring with harmless zero-divisors is atomic.*

In particular, Lemma 2.8 applies to $\mathbb{Z}_{p^n}[x]$:

2.9. Corollary. *$\mathbb{Z}_{p^n}[x]$ is atomic.*

3. Uniqueness of factorization

In the previous section we have seen that every non-zero non-unit of $\mathbb{Z}_{p^n}[x]$ is a product of irreducibles. Step by step we now reduce the task of factoring arbitrary elements of $\mathbb{Z}_{p^n}[x]$: first to factoring non-zerodivisors, then to factoring monic polynomials and, finally, to factoring monic primary polynomials. This is a matter of applying well-known facts of the "uniqueness" kind from [7] or [8]. It is only in the next section, concerned with factoring monic primary polynomials, that non-uniqueness of factorization comes into play.

Arbitrary polynomials to non-zerodivisors.

3.1. Lemma. *Let p be a prime and $n \geq 2$. For $f \in \mathbb{Z}_{p^n}[x]$, the following are equivalent:*

(1) *$f = pu$ for some unit u of $\mathbb{Z}_{p^n}[x]$.*

(2) *f is prime.*

(3) *f is irreducible and a zero-divisor.*

Proof. $(1 \Rightarrow 2)$. Let $v\colon \mathbb{Z}_{p^n}[x] \to N_n$ be p-adic valuation as defined in 1.1. Since $v(p) = 1$, additivity of v (1.2) implies that p is prime. Therefore every element associated to p is prime.

$(2 \Rightarrow 3)$. By Corollary 2.5, prime elements of $\mathbb{Z}_{p^n}[x]$ are irreducible. If c is prime, then $(c) \supseteq \mathrm{Nil}(\mathbb{Z}_{p^n}[x]) = (p)$; so $c \mid p$ and therefore c and p are associated. As p is a zero-divisor, so is c.

$(3 \Rightarrow 1)$. If c is a zero-divisor, then $c \in \mathrm{Z}(\mathbb{Z}_{p^n}[x]) = (p)$, meaning $c = pv$ for some v. If, furthermore, c is irreducible, then v must be a unit. □

3.2. Fact. Let $f \in \mathbb{Z}_{p^n}[x]$, $f \neq 0$.

(i) There exists a non-zerodivisor $g \in \mathbb{Z}_{p^n}[x]$, and $0 \leq k < n$, such that $f = p^k g$. Furthermore, k is uniquely determined by $k = v(f)$, and g is unique modulo (p^{n-k}).

(ii) In every factorization of f into irreducibles, exactly $v(f)$ of the irreducible factors are associates of p.

Proof. (i) follows from Fact 1.3 and the definition of p-adic valuation. (ii) follows from (i) and the fact that p is prime in $\mathbb{Z}_{p^n}[x]$ (by Lemma 3.1). □

Nonzerodivisors to monic polynomials.

3.3. Remark. ([7], Thm. XIII.6). Every non-zerodivisor $f \in \mathbb{Z}_{p^n}[x]$ is uniquely representable as $f = ug$, with u a unit of $\mathbb{Z}_{p^n}[x]$ and g monic. The degree of g is $\deg \bar{f}$, where $\bar{f}$ is the image of f in $\mathbb{Z}_p[x]$ under canonical projection.

Actually, McDonald [7] only shows the existence of g and u in 3.3, but uniqueness is easy: suppose $ug = vh$ with u, v units, g, h monic. Then $v^{-1}ug = h$. As g, h are monic, so is $v^{-1}u$. By 1.7, the only monic unit of $\mathbb{Z}_{p^n}[x]$ is 1, however, so $u = v$ and $g = h$.

Applying 3.3 to the irreducible factors of a non-zerodivisor of $\mathbb{Z}_{p^n}[x]$, we obtain:

3.4. Proposition. Let $f \in \mathbb{Z}_{p^n}[x]$, not a zero-divisor, and u and g the unique unit and monic polynomial, respectively, in $\mathbb{Z}_{p^n}[x]$ with $f = ug$. For every factorization $f = c_1 \cdot \ldots \cdot c_k$ into irreducibles, there exist uniquely determined monic irreducible $d_1, \ldots, d_k \in \mathbb{Z}_{p^n}[x]$ and units $v_1, \ldots, v_k$ in $\mathbb{Z}_{p^n}[x]$ with $c_i = v_i d_i$, $u = v_1 \cdot \ldots \cdot v_k$ and $g = d_1 \cdot \ldots \cdot d_k$.

By Proposition 3.4, we have reduced the question of factoring non-zerodivisors of $\mathbb{Z}_{p^n}[x]$ into irreducibles to the question of factoring monic polynomials into monic irreducibles. As there are only finitely many monic polynomials of each degree in $\mathbb{Z}_{p^n}[x]$, we also see that every non-zerodivisor of $\mathbb{Z}_{p^n}[x]$ has (up to associates) only finitely many factorizations into irreducibles.

Monic polynomials to primary monic polynomials.

3.5. Lemma. Let $f \in \mathbb{Z}_{p^n}[x]$, not a zero-divisor. Then (f) is a primary ideal of $\mathbb{Z}_{p^n}[x]$ if and only if the image of f under the canonical projection $\pi\colon \mathbb{Z}_{p^n}[x] \to \mathbb{Z}_p[x]$ is associated to a power of an irreducible polynomial.

Proof. In the principal ideal domain $\mathbb{Z}_p[x]$, the non-trivial primary ideals are precisely the principal ideals generated by powers of irreducible elements. The canonical projection π induces a bijective correspondence between primary ideals of $\mathbb{Z}_p[x]$ and primary ideals of $\mathbb{Z}_{p^n}[x]$ containing (p).

Now an ideal of $\mathbb{Z}_{p^n}[x]$ that does not consist only of zero-divisors is primary if and only if its radical is a maximal ideal (since the only non-maximal prime ideal is $(p) = \mathrm{Z}(\mathbb{Z}_{p^n}[x])$). Let $f \in \mathbb{Z}_{p^n}[x]$. Then, since every prime ideal of $\mathbb{Z}_{p^n}[x]$ contains (p), the radical of (f) is equal to the radical of $(f) + (p) = \pi^{-1}(\pi((f)))$.

For a non-zerodivisor f, therefore, (f) is primary if and only if $(f) + (p)$ is primary, which is equivalent to $\pi(f)$ being a primary element of $\mathbb{Z}_p[x]$. $\square$

3.6. Definition. We call a non-zerodivisor of $\mathbb{Z}_{p^n}[x]$ primary if its image under projection to $\mathbb{Z}_p[x]$ is associated to a power of an irreducible polynomial.

The simplest form of Hensel's Lemma shows that every monic $f \in \mathbb{Z}_{p^n}[x]$ is a product of primary polynomials. Furthermore, the monic primary factors of a monic polynomial in $\mathbb{Z}_{p^n}[x]$ are uniquely determined.

3.7. Remark. ([8], Thm. 13.8). Let $f \in \mathbb{Z}_{p^n}[x]$ monic, then there exist monic polynomials $f_1, \ldots, f_r \in \mathbb{Z}_{p^n}[x]$ such that $f = f_1 \cdot \ldots \cdot f_r$ and the residue class of f_i in $\mathbb{Z}_p[x]$ is a power of a monic irreducible polynomial $g_i \in \mathbb{Z}_p[x]$, with $g_1, \ldots, g_r$ distinct. The polynomials $f_1, \ldots, f_r \in \mathbb{Z}_{p^n}[x]$ are (up to ordering) uniquely determined.

3.8. Proposition. *Every non-zero polynomial $f \in \mathbb{Z}_{p^n}[x]$ is representable as*

$$f = p^k u f_1 \ldots f_r$$

with $0 \leq k < n$, u a unit of $\mathbb{Z}_{p^n}[x]$, $r \geq 0$, and $f_1, \ldots, f_r \in \mathbb{Z}_{p^n}[x]$ monic polynomials such that the residue class of f_i in $\mathbb{Z}_p[x]$ is a power of a monic irreducible polynomial $g_i \in \mathbb{Z}_p[x]$, and $g_1, \ldots, g_r$ are distinct.

Moreover, $k \in \mathbb{N}_0$ is unique, $u \in \mathbb{Z}_{p^n}[x]$ is unique modulo $p^{n-k}\mathbb{Z}_{p^n}[x]$, and also the f_i are unique (up to ordering) modulo $p^{n-k}\mathbb{Z}_{p^n}[x]$.

Proof. Follows from 3.2, 3.4 and 3.7. $\square$

For the the monoid of non-zerodivisors of $\mathbb{Z}_{p^n}[x]$ this means:

3.9. Theorem. *Let M be the multiplicative monoid of non-zerodivisors of $\mathbb{Z}_{p^n}[x]$, and U its group of units. Let M' be the submonoid of M consisting of all monic polynomials. Then*

$$M \simeq U \oplus M'.$$

For every monic irreducible polynomial $f \in \mathbb{Z}_p[x]$ let M_f be the submonoid of M' consisting of those monic polynomials $g \in \mathbb{Z}_{p^n}[x]$ whose image under projection to $\mathbb{Z}_p[x]$ is a power of f. Then

$$M' \simeq \sum_f M_f$$

where f ranges through all monic irreducible polynomials of $\mathbb{Z}_p[x]$.

Proof. Follows by specializing 3.8 to non-zerodivisors, which by 1.3 are exactly the elements of $\mathbb{Z}_{p^n}[x]$ not divisible by p. $\square$

The example in the introduction shows that the monoid M_x (corresponding to the irreducible polynomial $x \in \mathbb{Z}_p[x]$) has infinite elasticity (defined in 4.1 below). We will show this of each of the direct summands M_f in Theorem 3.9.

4. Non-uniqueness of factorization and infinite elasticity

Irreducible elements are defined in an arbitrary monoid in the same way as we defined them for the multiplicative monoid of a ring in 2.1. Note that the monoid of non-zerodivisors of $\mathbb{Z}_{p^n}[x]$, and its submonoid the monoid of all monic polynomials in $\mathbb{Z}_{p^n}[x]$ are cancellative.

4.1. Definition. Let $(M, \cdot)$ be a cancellative monoid.

(1) For $k \geq 2$, let $\rho_k(M)$ be the supremum of all those $m \in \mathbb{N}$ for which there exists a product of k irreducibles that can also be expressed as a product of m irreducibles.

(2) The *elasticity* of M is $\sup_{k\geq 2}(\rho_k(M)/k)$; in other words, the elasticity is the supremum of the values m/k such that there exists an element of M that can be expressed both as a product of k irreducibles and as a product of m irreducibles.

4.2. Lemma. *Let f be a monic polynomial in $\mathbb{Z}[x]$ which represents an irreducible polynomial in $\mathbb{Z}_p[x]$. Let $d = \deg(f)$. Let $n, k \in \mathbb{N}$ with $0 < k < n$, $m \in \mathbb{N}$ with $\gcd(m, kd) = 1$, and $c \in \mathbb{Z}$ with $p \nmid c$. Then*

$$f(x)^m + cp^k$$

represents an irreducible polynomial in $\mathbb{Z}_{p^n}[x]$.

Proof. Suppose otherwise. Then there exist $g, h, r \in \mathbb{Z}[x]$, with g, h monic, g irreducible in $\mathbb{Z}_{p^n}[x]$, such that

$$f(x)^m + cp^k = g(x)h(x) + p^n r(x)$$

and $0 < \deg g < dm$. In $\mathbb{Z}_p[x]$, g is a power of f, by unique factorization. Therefore $\deg g = ds$ with $0 < s < m$.

Let α be a zero of g. Let R be the ring of algebraic integers in $\mathbb{Q}[\alpha]$ and P a prime of R above p with ramification index e. Let v be the normalized valuation on $\mathbb{Q}[\alpha]$ corresponding to P.

Since $f(\alpha)^m = p^n r(\alpha) - cp^k$, we have $v(f(\alpha)) = ke/m$. As m is relatively prime to k, m divides e. This holds for the ramification index e_i of every prime P_i of R above p. Let f_i be the inertia degree of P_i. Then m divides $\sum_i e_i f_i = [\mathbb{Q}[\alpha] : \mathbb{Q}] = \deg g = ds$. As m is relatively prime to d, m divides s, a contradiction to $0 < s < m$. $\square$

4.3. Theorem. *Let $n \geq 2$. Let f be a monic irreducible polynomial in $\mathbb{Z}_p[x]$. Let M_f be the submonoid of the multiplicative monoid of $\mathbb{Z}_{p^n}[x]$ defined in Theorem 3.9.*

Then the elasticity of M_f is infinite. Moreover, $\rho_2(M_f) = \infty$.

Proof. In the proof, f will, by abuse of notation, denote a monic polynomial in $\mathbb{Z}[x]$ which under canonical projection to $\mathbb{Z}_p[x]$ maps to the f in the theorem.

Let q be a prime with $q > \max(n-1, \deg f)$. By Lemma 4.2, $f(x)^q + p^{n-1}$ is irreducible in $\mathbb{Z}_{p^n}[x]$, and

$$\left(f(x)^q + p^{n-1}\right)^2 = f(x)^q(f(x)^q + 2p^{n-1})$$

is an example of factorization of a polynomial in M_f into either 2 irreducible factors - on the left - or more than q irreducible factors - on the right (actually, the number of irreducible factors on the right is $q+1$ for $p \neq 2$, by Lemma 4.2, and $2q$ for $p = 2$.) As q can be made arbitrarily large, $\rho_2(M_f) = \infty$, and the elasticity of M_f is infinite. $\square$

4.4. Corollary. *Let M be the multiplicative monoid of non-zerodivisors of $\mathbb{Z}_{p^n}[x]$ and M' the submoinoid of monic polynomials. Then the elasticity of M' is infinite, and $\rho_2(M') = \infty$. Therefore the elasticity of M is infinite and also $\rho_2(M) = \infty$.*

Proof. Indeed, by Theorem 3.9 and Theorem 4.3, M' is an infinite direct sum of monoids M_f of infinite elasticity and satisfying $\rho_2(M_f) = \infty$. $\square$

Acknowledgment. The authors wish to thank F. Halter-Koch for useful comments.

References

[1] A. G. Ağargün, D. D. Anderson, and S. Valdes-Leon, *Factorization in commutative rings with zero divisors. III.*, Rocky Mountain J. Math. 31 (2001), 1–21.

[2] D. D. Anderson and S. Valdes-Leon, *Factorization in commutative rings with zero divisors.*, Rocky Mountain J. Math. 26 (1996), 439–480.

[3] D. D. Anderson and S. Valdes-Leon, *Factorization in commutative rings with zero divisors. II.*, in Factorization in integral domains (Iowa City Conf.

1996), D. D. Anderson, ed., vol. 189 of Lect. Notes Pure Appl. Math., Marcel Dekker, 1997, 197–219.

[4] S. Frisch, *Polynomial functions on finite commutative rings*, in Advances in commutative ring theory (3rd Fez Conf. 1997), D. Dobbs et al., eds., vol. 205 of Lect. Notes Pure Appl. Math., Marcel Dekker, 1999, 323–336.

[5] A. Geroldinger and F. Halter-Koch, *Non-unique factorizations. Algebraic, combinatorial and analytic theory*, Chapman&Hall/CRC, 2006.

[6] J. J. Jiang, G. H. Peng, Q. Sun, and Q. F. Zhang, *On polynomial functions over finite commutative rings*, Acta Math. Sin. (Engl. Ser.) 22 (2006), 1047–1050.

[7] B. R. McDonald, *Finite rings with identity*, Marcel Dekker, 1974.

[8] Z.-X. Wan, *Lectures on finite fields and Galois rings*, World Scientific, 2003.

[9] Q. F. Zhang, *Polynomial functions and permutation polynomials over some finite commutative rings*, J. Number Th. 105 (2004), 192–202.

Institut für Mathematik A
Technische Universität Graz
Steyrergasse 30
A-8010 Graz, Austria

Phone +43 316 873 7133
Fax +43 316 873 107133

Ch. F.
cfrei@sbox.TUGraz.at

S. F.
frisch@blah.math.tu-graz.ac.at