Master in Mathematics

University of Luxembourg

Student Project

Factorisation of polynomials over $\mathbb{Z}/p^n\mathbb{Z}[x]$

Author : **Salima LAMHAR**

Supervisors : **Pr.Gabor WIESE - Dr.Panagiotis TSAKNIAS**

Contents

1 Introduction

1.1 Setting

In this subject based on the article [1], we will study the phenomena of factorization of polynomials into irreducibles over $\mathbb{Z}/p^n\mathbb{Z}[x]$. Indeed if the factorisation is unique over $\mathbb{Z}/p\mathbb{Z}$ (p prime), it's far from being the same over $\mathbb{Z}/p^n\mathbb{Z}[x]$.

We will show that the elasticity of the multiplicative monoid of monic polynomials in $\mathbb{Z}/p^n\mathbb{Z}[x]$ is infinite since it is a direct sum of monoids corresponding to irreducible polynomials in $\mathbb{Z}/p\mathbb{Z}[x]$ and that each of these monoids has infinite elasticity.

By using a few properties concerning uniqueness of some kinds of factorizations of polynomials over $\mathbb{Z}/p^n\mathbb{Z}[x]$, we can generalize the non-uniqueness of factorization into irreducibles to arbitrary non-zero polynomials. In fact, we can reduce the question of factoring arbitrary non-zero polynomials into irreducibles to the problem of factoring monic polynomials into monic irreducibles.

Throughout this paper, p is prime and $n \geq 2$ (p denotes also its residue class in $\mathbb{Z}/p^n\mathbb{Z}$ or in $\mathbb{Z}/p^n\mathbb{Z}[x]$). Π defines the canonical projection from $\mathbb{Z}/p^n\mathbb{Z}[x]$ to $\mathbb{Z}/p\mathbb{Z}[x]$.
M is the multiplicative cancellative monoid of non-zerodivisors of $\mathbb{Z}/p^n\mathbb{Z}[x]$.

1.2 Unique factorization over $\mathbb{Z}/p\mathbb{Z}[x]$

Let R be a commutative ring and let us define :

$$T=\{u \in R \mid u \text{ is an unit }\} \cup \{p_1...p_n \in R \mid p_i \text{ is prime and } n \in N\}$$

Theorem 1.1 (Kaplansky) : *An integral domain R is a UFD if and only if every non-zero prime ideal in R contains a prime element.*

Proof: If R is a field the proof in trivial since the only ideals are (0) and R.
($\Rightarrow$) Let P be a non-zero prime ideal, then P is proper and there is non-zero $x \in P$ which is not a unit. Since x is not a unit and $x \in T$, there are prime elements $p_1, \ldots, p_k \in R$ such that $x = p_1....p_k$ (R is a UFD if and only if $T = R \setminus \{0\}$). Since P is prime $\exists i$ such that $p_i \in P$.
($\Leftarrow$) Assume that R is not a UFD. Then there is a non zero $x \in R$ such that $x \notin T$. Consider the ideal (x). We will show, that $(x) \cap T = \emptyset$. Assume that there is $r \in R$ such that $r.x \in T$. Then it follows that $x \in T$ (since if $a, b \in R$ are such that $a.b \in T$, then both $a, b \in T$) which is a contradiction.
Since $(x) \cap T = \emptyset$ and T is a multiplicative subset, there is a prime ideal P in R such that $(x) \subseteq P$ and $P \cap T = \emptyset$. Since we assumed that every non-zero prime ideal contains prime element (and P is nonzero, since $x \in P$),we obtain a contradiction, which completes the proof. □

Theorem 1.2 : *Every principal ideal domain is a unique factorization domain.*

Proof: Recall that, due to **Kaplansky Theorem** it is enough to show that every non-zero prime ideal in R contains a prime element.
On the other hand, recall that an element $p \in R$ is prime if and only if the ideal (p) generated by p is non-zero and prime.
Thus if P is a nonzero prime ideal in R, then (since R is a PID) there exists $p \in R$ such that $P = (p)$. This completes the proof. □
We conclude then, that $\mathbb{Z}/p\mathbb{Z}[x]$ is a unique factorization domain since it is a PID.

Example 1.3 : In $\mathbb{Z}/3\mathbb{Z}[x]$, $Q = x^3 + x^2 + x$ then $Q = x.(x + 2)^2$ is the unique factorization into irreducibles of Q.

1.3 An example of the phenomema over $\mathbb{Z}/p^n\mathbb{Z}[x]$

$$(x^m + p^{n-1})^2 = x^m(x^m + 2.p^{n-1})$$

Consider the equality above. Let us assume that the concept of irreducibility in $\mathbb{Z}/p^n\mathbb{Z}[x]$ is analogous to the concept of irreducibility in integral domains and that $\mathbb{Z}/p^n\mathbb{Z}[x]$ is atomic (every element has a factorization into irreducible elements).
By using the unique factorization in $\mathbb{Z}/p\mathbb{Z}[x]$, we can prove that $(x^m + p^{n-1})$ is a product of at most $(n-1)$ irreducibles. Indeed, this polynomial represents a power of x in $\mathbb{Z}/p\mathbb{Z}[x]$, then by unique factorization each of their factors in $\mathbb{Z}/p^n\mathbb{Z}[x]$ must represent a power of x in $\mathbb{Z}/p\mathbb{Z}[x]$(apart from units since $(\mathbb{Z}/p\mathbb{Z})^* = (\mathbb{Z}/p\mathbb{Z}[x])^*$ and a polynomial in $\mathbb{Z}/p^n\mathbb{Z}[x]$ is a unit if and only if it maps to a unit in $\mathbb{Z}/p\mathbb{Z}[x]$ under the canonical projection Π). Then, the constant coefficient of every such factor is divisible by p. Since $(x^m + p^{n-1})$ is divisible by no higher power of p than $n-1$, $(x^m + p^{n-1})^2$ is divisible by no higher power of p than $2(n-1)$.
Hence, for arbitrary $m \in \mathbb{N}$, there exists in $\mathbb{Z}/p^n\mathbb{Z}[x]$ a product of at most $2(n-1)$ irreducibles that is also representable as a product of more than m irreducibles without any condition on m.

2 Definition of the elasticity and non-uniqueness of factorization of some monic polynomials

Definition 2.1 : Suppose that S is a set and (.) is some binary operation $S \times S \to S$, then S with (.) is a monoid if it satisfies the following two axioms:
-Associativity: For all a, b and c in S, the equality $(a.b).c = a.(b.c)$ holds.
-Identity element: there exists an element e in S such that for every element a in S, the equations $e.a = a.e = a$ hold.
In other words, a monoid is a semigroup with an identity element.

Definition 2.2 : A submonoid of a monoid $(S, .)$ is a subset N of S that is closed under the monoid operation and contains the identity element e of S. In other words, N is a submonoid of S if $N \subseteq S$ and $x.y \in N$ whenever $x, y \in N$ and $e \in N$.

Definition 2.3 : Let $(S, .)$ be a semigroup together with a partial order $\leqslant$. We say that his order is compatible with the semigroup operation, if $x \leqslant y \Rightarrow t.x \leqslant t.y$ and $x.t \leqslant y.t$ for all $x, y, t \in S$.

Definition 2.4 : Let S be a semigroup. An element $a \in S$ is left cancellative (respectively right cancellative) if $a.b = a.c$ implies $b = c$ for all b and c in S (respectively if $ba = ca$ implies $b = c$). If every element in S is both left cancellative and right cancellative, then S is called a cancellative semigroup.

Definition 2.5 : Let $(S, .)$ be a cancellative monoid.
(i) For $k \geq 2$, let $\phi_k(S)$ 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.
(ii) The elasticity of S is $\underset{k \geqslant 2}{sup}(\frac{\Phi_k(M)}{k})$, in other words, the elasticity is the supremum of the values $\frac{m}{k}$ 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.

Lemma 2.6 : *Let f be a monic polynomial in $\mathbb{Z}/p^n\mathbb{Z}[x]$ which maps to an irreducible polynomial in $\mathbb{Z}/p\mathbb{Z}[x]$. Let $d = deg(f)$. Let $n, k \in N$ with $0 < k < n$ and $m \in N$ with $gcd(m, kd) = 1$ and $c \in Z$ with $p \nmid c$. Then:*

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

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

Proof: Suppose otherwise. Then $\exists\ g, h, r \in \mathbb{Z}[x]$, with g, h monic and g irreducible in $\mathbb{Z}/p^n\mathbb{Z}[x]$, such that:

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

and $0 < deg\ g < dm$. By using the unique factorization in $\mathbb{Z}/p\mathbb{Z}[x]$, g is a power of f modulo p. Therefore, $deg\ g = ds$ with $0 < s < m$. Let α be a zero of g. Let A be the ring of algebraic integers in $Q[\alpha]$. Then by 'Splitting of prime ideals in Galois extensions' we have that $pA = P_1^{e_1}...P_r^{e_r}$ and $[Q[\alpha] : Q] = \sum_i e_i.[A/P_i : \mathbb{Z}/p\mathbb{Z}] = deg\ g = ds$. Let $w^*_{P_1}$ the normalized valuation on $Q[\alpha]$ corresponding to P_1 (see section 3,3.1). Since $f(\alpha)^m = p^n r(\alpha) - cp^k$, we have $m.w^*_{P_1}(f(\alpha)) = ke_1$. As m is relatively prime to k, m divides e_1. By the same reasoning, we have that m divides e_i for $i \in 1, ..., r$ then m divides $deg\ g = [Q[\alpha] : Q] = \sum_i e_i.[A/P_i : \mathbb{Z}/p\mathbb{Z}] = ds$. As m is relatively prime to d, m divides s, which is a contradiction since $0 < s < m$. □

Theorem 2.7 : *Let $n \geq 2$. Let f be a monic irreducible polynomial in $\mathbb{Z}/p\mathbb{Z}[x]$. Let M_f be the submonoid of the multiplicative monoid M consisting of those monic polynomials $g \in \mathbb{Z}/p^n\mathbb{Z}[x]$ whose image under Π is a power of f. Then the elasticity of M_f is infinite . Moreover, $\Phi_2(M_f) = \infty$.*

Proof: Let us, by abuse of notation, denote by g a monic polynomial in $\mathbb{Z}/p^n\mathbb{Z}[x]$ which maps under Π to the irreducible polynomial f in $\mathbb{Z}/p\mathbb{Z}[x]$.
Let q be a prime with $q > max(n-1, deg(g))$. By **Lemma 2.6**, $g(x)^q + p^{n-1}$ is irreducible in $\mathbb{Z}/p^n\mathbb{Z}[x]$. Let us consider the equality:

$$(g(x)^q + p^{n-1})^2 = g(x)^q(g(x)^q + 2.p^{n-1})$$

This is an example of factorization of a polynomial in M_f into (on the left) 2 irreducible factors and by using the **Lemma 2.6**, (on the right) $q+1$ irreducible factors (if $p \neq 2$) and $2q$ (if $p = 2$). As q can be made arbitray large, then $\phi_2(M_f) = \infty$ and the elasticity of M_f is infinite. □

Since M_f is fully elastic, we conclude that the factorization of monic polynomials (whose image under Π is a power of an irreducible) into irreducibles over $\mathbb{Z}/p^n\mathbb{Z}[x]$ is not unique. The aim is now to generalize the result to all monic polynomials and then to non-zerodivisors and then to arbitrary polynomials.

3 Commutative rings with harmless zero-divisors

Definition 3.1 : We extend p-adic valuation to $\mathbb{Z}[x]$ by $v^*(f) = min_k v(a_k)$ where v is the usual p-adic valuation on $\mathbb{Z}$ and $f = \sum_k a_k x^k$.
v^* defines a surjective mapping $v^* : \mathbb{Z}[x] \to \mathbb{N}_0 \cup \{\infty\}$. Let us denote by $(\mathbb{N}_n, +, \leqslant)$ the ordered monoid with elements $0, 1, ..., n-1, \infty$, resulting from factoring $(\mathbb{N}_0 \cup \{\infty\}, +, \leqslant)$ by the congruence relation that identifies all values greater or equal than n, including ∞, by abuse of notation, we will use v^* for the surjective mapping $v^* : \mathbb{Z}/p^n\mathbb{Z}[x] \to \mathbb{N}_n$ obtained by factoring p-adic valuation $v^* : Z[x] \to \mathbb{N}_0 \cup \{\infty\}$ by the same congruence relation. Indeed, $v^* : \mathbb{Z}/p^n\mathbb{Z}[x] \to \mathbb{N}_n$ behaves like a valuation, except that $(\mathbb{N}_n, +)$ is not a group and cannot be extended to a group, as it is not cancellative.

Proposition 3.2: *$v^* : \mathbb{Z}/p^n\mathbb{Z}[x] \to \mathbb{N}_n$ satisfies:*
(i) $v^*(f) = \infty \iff f = 0$.
(ii) $v^*(f+g) \geqslant min(v^*(f), v^*(g))$.
(iii) $v^*(fg) = v^*(f) + v^*(g)$.

Proposition 3.3 : *For $f \in \mathbb{Z}/p^n\mathbb{Z}[x]$, the following are equivalent:*
(i) $v^*(f) > 0$ (all coefficients of f are divisible by p).
(ii) f is nilpotent.
(iii) f is a zero-divisor.

Proof:
$(i) \Rightarrow (ii)$ Let us consider $f = \sum_k a_k x^k$. Since $v^*(f) > 0$ all the coefficients of are divisible by p. Then, $f = \sum_k p.a'_k x^k$ such that for each k, $a_k = p.a'_k$. Then $f = p.(\sum_k a'_k x^k)$, and $f^n = p^n.(\sum_k a'_k x^k)^n = 0$. Therefore f is nilpotent.
$(ii) \Rightarrow (iii)$ Let us asume that f is nilpotent. Then $\exists k \in \mathbb{N}$ such that $f^k = 0$ and $f^{k-1} \neq 0$. Then $f.f^{k-1} = 0$ and f is a zero-divisor ($f \neq 0$).
$(iii) \Rightarrow (i)$ Let us consider $f \in \mathbb{Z}/p^n\mathbb{Z}[x]$ such that f is a zero-divisor then $\exists g \in \mathbb{Z}/p^n\mathbb{Z}[x]$ such that $g \neq 0$ and $f.g = 0$. Then the lift of $f.g$ in $\mathbb{Z}[x]$ is a multiple of p^n . Then by using properties of v^* in $\mathbb{Z}[x]$, we have $v^*(\overline{f.g}) = v^*(\overline{f}.\overline{g}) = v^*(\overline{f}).v^*(\overline{g}) = n$. Since $g \neq 0$, we have $v^*(\overline{g}) < n$. So we conclude that $v^*(\overline{f}) > 0$ and $v^*(f) > 0$. □

Definition 3.4 : Let R be a commutative ring.
(i) $Nil(R)$ denotes the nilradical of R, *i.e.* the set $\{r \in R, \exists n \in N, r^n = 0\}$.
(ii) $J(R)$ denotes the Jacobson radical of R, *i.e.* the intersection of all maximal ideals of R.
(iii) $Z(R)$ denotes the set of zero-divisors of R.

Proposition 3.5 : $Nil(R) = \{r \in R, \exists n \in N, r^n = 0\} = \underset{P prime}{\cap} P$

Proof:
$(\subseteq)$: Let $r \in Nil(R)$, then $\exists n \in N$ such that $r^n = 0 \in P$ (P prime). Since P is prime we have $r \in P$, and $r \in \underset{P prime}{\cap} P$.
$(\supseteq)$: Let $r \in \underset{P prime}{\cap} P$, and let us suppose that $r \notin Nil(R)$. Let E be the set of ideals which contain no power of r. E is non-empty, because E contains (0). By using Zorn's lemma, E has a maximal ideal, let us denote it by P. Then P contains no power of r and $P \subsetneq R$. Let us now show that P is prime. Consider $x, y \notin P$ such that $xy \in P$.
$x \notin P \Rightarrow P \subsetneq P + R.x$. But P is maximal in E, then $P + R.x \notin E$ and contains a power of r. Hence $\exists k > 0$, $q \in P$ and $s \in R$ such that $r^k = q + s.x$. By the same reasoning, $\exists l > 0$, $q' \in P$ and $t \in R$ such that: $r^l = q' + ty$. By using these equalities, we have:

$$r^{k+l} = qq' + q(ty) + q'(sx) + (st)xy$$

We remark that $r^{k+l} \notin P$ but $qq' + q(ty) + q'(sx) + (st)xy \in P$ which is a contradiction. Then $x \in P$ or $y \in P$ and P is prime. This completes the proof and $r \in Nil(R)$. $\square$

Proposition 3.6 : *Let Q be a maximal ideal of $\mathbb{Z}[x]$, then Q is of the form:*

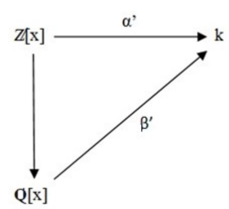
$$Q = (p, f(x))$$

Where $f \in \mathbb{Z}[x]$ such that f represents an irreducible polynomial in $\mathbb{Z}/p\mathbb{Z}[x]$.

Proof: Let us consider Q an arbitrary maximal ideal of $\mathbb{Z}[x]$, and denote by K the quotient ring $\mathbb{Z}[x]/Q$ which is a field. Consider $\theta : \mathbb{Z} \to K$ the composition of the two natural maps :

$$\alpha : \mathbb{Z} \hookrightarrow \mathbb{Z}[x]$$
and
$$\alpha' : \mathbb{Z}[x] \to K$$

θ is not injective. Suppose θ is injective, then, since K is a field, θ extends to an injection $\theta' : \mathbb{Q} \hookrightarrow K$ and then α' to a homomorphism $\beta' : \mathbb{Q}[x] \to K$



The map β' is clearly surjective, since α' already is. Now, if β' is injective, we will have an isomorphism $\mathbb{Q}[x] \simeq K$, but $\mathbb{Q}[x]$ is not a field. Therefore, $Ker(\beta') = (g(x))$ for a non-zero polynomial g, which must be then irreducible. By replacing g with a non-zero constant multiple, we can assume that g is primitive polynomial in $\mathbb{Z}[x]$. We thus have an isomorphism $\mathbb{Q}[x]/(g) \simeq K$. But this will imply that the natural map $\mathbb{Z}[x] \hookrightarrow \mathbb{Q}[x]$ induces a surjection $\mathbb{Z}[x] \to \mathbb{Q}[x]/(g)$ which will induce an isomorphism $\mathbb{Z}[x]/(g) \simeq \mathbb{Q}[x]/(g)$, let us show that is a contradiction. If we consider $g(x) = a_n x^n + a_{n-1}x^{n-1} + ... + a_1 x + a_0$ (with $a_n \neq 0$), then we have in $\mathbb{Q}[x]/(g)$:

$$a_n \overline{x}_n + a_{n-1}\overline{x}_{n-1} + ... + a_0 = 0$$

So we can write,

$$\overline{x}^n = (\tfrac{-a_{n-1}}{a_n})\overline{x}^{n-1} + ... + (\tfrac{-a_1}{a_n})\overline{x} + (\tfrac{-a_0}{a_n})$$

Then $\overline{x}^n$ can be written as linear combination of lower powers with coefficients in $\mathbb{Z}[\frac{1}{a_n}]$. Using this and an easy induction, we deduce that any polynomial in $\mathbb{Q}[x]/(g)$ can be written as linear combination of elements in the set $B = \{1, \overline{x}, \overline{x}^2, ..., \overline{x}^{n-1}\}$. It is clear that $\sum\limits_{i\in\{0..n-1\}} c_i\overline{x}^i = 0$ implies that $\sum\limits_{i\in\{0..n-1\}} c_i x^i \in (g(x))$ (B is linearly independent in $\mathbb{Q}[x]/(g)$). By examining degrees, we must have $c_i = 0$ for all i. Now, take p prime that does not divide a_n. Then $\frac{1}{p}$ cannot be spanned by B with coefficients in $\mathbb{Z}[\frac{1}{a_n}]$. We know now that θ is not injective and then $Ker(\theta) = (n)$ for some n non-zero. However, since the image of θ is an integral domain, n must be a prime p. Therefore, we must have $p \in Q$ for some prime p. We know that the maximal ideals in $\mathbb{Z}[x]$ that contain p are in bijection with the maximal ideals in $\mathbb{Z}[x]/(p) \simeq \mathbb{Z}/p\mathbb{Z}[x]$. So $Q/(p) = (f_0(x))$ for an irreducible polynomial $f_0 \in \mathbb{Z}/p\mathbb{Z}[x]$. But then $Q = (p, f(x))$ for any lift f of f_0, as was to be shown. □

Proposition 3.7 : $Nil(\mathbb{Z}/p^n\mathbb{Z}[x]) = J(\mathbb{Z}/p^n\mathbb{Z}[x]) = (p) = Z(\mathbb{Z}/p^n\mathbb{Z}[x])$

Proof: By **Proposition3.3** we have $(p) = Nil(\mathbb{Z}/p^n\mathbb{Z}[x]) = Z(\mathbb{Z}/p^n\mathbb{Z}[x])$. Let us now prove that $J(\mathbb{Z}/p^n\mathbb{Z}[x]) = (p)$. We know by **Proposition 3.6** that the ideals (p, f) with f representing an irreducible polynomial in $\mathbb{Z}/p\mathbb{Z}[x]$ are precisely the maximal ideals of $\mathbb{Z}[x]$. Let us denote by λ the canonical projection from $\mathbb{Z}[x]$ into $\mathbb{Z}/p^n\mathbb{Z}[x]$. Consider J a maximal ideal of $\mathbb{Z}/p^n\mathbb{Z}[x]$, then $\lambda^{-1}((J))$ is a maximal ideal of $\mathbb{Z}[x]$. Then $\lambda^{-1}((J)) = (p, f)$ with f irreducible modulo p. Then $J = \lambda(\lambda^{-1}(J)) = \lambda((p, f)) = (p, f)$. Then $J(\mathbb{Z}/p^n\mathbb{Z}[x]) = \bigcap\limits_i (p, f_i) = (p)$ such that f_i represents an irreducible polynomial in $\mathbb{Z}/p\mathbb{Z}[x]$. □

Definition 3.8 : Let R be a commutative ring. Let $a, b \in R$, $c \in R$ a non-zero non-unit. We say that:
(i) c is weakly irreducible if: $c = ab \Longrightarrow c \mid a$ or $c \mid b$.
(ii) a and b weakly associated if $a \mid b$ and $b \mid a$ (or equivalently $(a) = (b)$).
(iii) R is atomic (respectively weakly atomic) if every non-zero non-unit is a product of irreducibles (respectively weakly irreducibles) elements.

Definition 3.9 : Let R be a commutative ring. We say that R is a ring with harmless zero-divisors if $Z(R) \subseteq 1 - U(R) = \{1 - u \mid u \text{ an unit of } R\}$.

Lemma 3.10 : *R be a ring with harmless zero-divisors and $a, b, c, u, v \in R$. Then:*
(i) if $a \neq 0$, $a = bu$ and $b = av$ then u, v are units.
(ii) a, b are weakly associated if and only if they are associated.
(iii) c is weakly irreducible if and only if c is irreducible.
(iv) if c is prime, then c is irreducible.

Proof: (i) Let us consider $a = bu$ and $b = av$ with $a \neq 0$. Then $a(1 - vu) = 0$ then $(1 - vu)$ is a zero-divisor, then $\exists w$ a unit such that $1 - vu = 1 - w$ then $vu = w$ and u, v are units.
(ii) we have $a \mid b$ and $b \mid a \Longleftrightarrow \exists u, v$ such that $a = bu$ and $b = av$ then by (i) u and v are units then a and b are associated.
(iii) Suppose that $c = ab$ since c is weakly irreducible then $c \mid a$ or $c \mid b$, $\exists u, v$ such that $a = cu$ or $b = cv$ then by (i) u, b are units or v,a are units.
(iv) Let $c = ab$ then $c \mid ab$. Since c is prime $c \mid a$ or $c \mid b$ then c is weakly irreducible and then irreducible. □

Corollary 3.11 : *If a commutative ring R satisfies $Z(R) \subseteq J(R)$ then the statements of the **Lemma 3.10** hold.*

Proof: Let us first prove that for any commutative ring R, $J(R) \subseteq 1 - U(R)$. Let us consider $x \in J(R)$ such that $1 - x$ is a non-unit, then $\exists S$ a maximal ideal such that $1 - x \in S$. Since $J(R)$ is the intersection of all maximal ideals, $x \in S$ and then $1 = (1 - x) + x \in S$. This is a contradiction. By using this result, we have that $Z(R) \subset J(R) \subset 1 - U(R)$ and then every commutative ring such that $Z(R) \subset J(R)$ is a ing with harmless zero-divisors. □

Proposition 3.12 : $\mathbb{Z}/p^n\mathbb{Z}[x]$ *is a ring with harmless zero-divisors.*

Proof: Directly from the **Proposition 3.7** and **Corollary 3.11**. □

Definition 3.13 : We say that a commutative ring R satisfies the ascending chain condition for principal ideals (ACCP) if there is no infinite strictly ascending chain of principal ideals.

Theorem 3.14 : *If R is a commutative ring which satisfies ACCP then R is weakly atomic.*

Proof: Let us suppose that there exists $r \in R$ such that r non-zero non-unit that cannot be expressed as a product of weakly irreducible elements. Then r is not weakly irreducible and $\exists a, b$ such that at least one of them is non-zero non-unit (since r is non-zero non unit) with $r = ab$. Suppose that a is non-zero non unit, $a \mid r$ and $r \nmid a$ then $(r) \subsetneqq (a)$. By iteration on (a) we obtain (c) (with c non-unit non-zero) such that $(r) \subsetneqq (a) \subsetneqq (c)$ and so on... We get then an infinite ascending chain of principal ideals which is a contradiction. □

Lemma 3.15 : *Every commutative ring with harmless zero-divisors satisfying ACCP is atomic.*

Proof: By using the **Theorem 3.14** we have that every commutative ring with ACCP is weakly atomic, every non-zero non-unit is a product of weakly irreducible elements. By **Lemma 3.9** every such factor is irreducible then we obtain a product of irreducible elements. □

Corollary 3.16 : $\mathbb{Z}/p^n\mathbb{Z}[x]$ *is atomic.*

In this section, we proved that in commutative rings the concept of harmless zero-divisors permits to avoid the problems with defining the concepts of irreducibility and primality which appear as soon as zero-divisors are engaged. Then we establish a relationship between 'weaker' concepts (weakly irreductible, weakly associative) and 'stronger' ones, especially for $\mathbb{Z}/p^n\mathbb{Z}[x]$. Therefore, we will be interested particulary in the non-zerodivisors, then in monic polynomials and finally in the monic primary polynomials.

4 Uniqueness of some kinds of factorizations over $\mathbb{Z}/p^n\mathbb{Z}[x]$

4.1 Arbitrary polynomials to non-zerodivisors

Lemma 4.1 : *Let $f \in \mathbb{Z}/p^n\mathbb{Z}[x]$. Then the following are equivalent:*
(i) $f = pu$ for some $u \in U(\mathbb{Z}/p^n\mathbb{Z}[x])$
(ii) f is prime
(iii) f is irreducible and a zero-divisor

Proof:
$(i) \Rightarrow (ii)$ p is prime in $\mathbb{Z}/p^n\mathbb{Z}[x]$ (since $v^*(p) = 1$), f is asociated to p, then f is prime as well.
$(ii) \Rightarrow (iii)$ by **Lemma 3.9** f is prime then f is irreducible. Moreover the ideal (f) is prime and by **Propositon 3.6** $(p) = Nil(\mathbb{Z}/p^n\mathbb{Z}[x]) \subseteq (f)$ then $f \mid p$ and p and f are associated. Since p is a zero-divisor, f is a zero-divisor as well.
$(iii) \Rightarrow (i)$ f is a zero-divisor, then $(f) \subseteq Z(\mathbb{Z}/p^n\mathbb{Z}[x]) = (p)$, then $\exists u \in \mathbb{Z}/p^n\mathbb{Z}[x]$ such that $f = pu$. Moreover, f is irreducible then u must be a unit. □

Proposition 4.2 :
(i) Let $f \in \mathbb{Z}/p^n\mathbb{Z}[x]$ a non-zero polynomial,there exists a non-zerodivisor g and $0 \leqslant k \leqslant n$, 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 factorisation of f into irreducibles, we have exactly $v^*(f)$ factors associated to p.

Proof:
(i) We have by **Proposition 3.3** if f is a zero-divisor, $k = v^*(f) > 0$, if not $k = v^*(f) = 0$. Moreover, $\exists g \in \mathbb{Z}/p^n\mathbb{Z}[x]$ such that $f = p^k g$. Uniqueness of g: let us assume that it exists g' which satisfies the same condition, and $g \neq g'$ we have in $\mathbb{Z}[x]$: $f = p^k g = p^k g' \Rightarrow p^k(g - g') = 0$ then by using the properties of the p-adic valuation we have:
$v^*(p^k(g-g')) = v^*(p^k) + v^*(g-g') = k + v^*(g-g') = n$ then $v^*(g-g') = n-k$ but we have $v^*(g-g') \leqslant min(v^*(g), v^*(g')) = 0$ then $n = k$ and $f = 0$ (in $\mathbb{Z}/p^n\mathbb{Z}[x]$). Contradiction.
(ii) It follows directly from (i) since we have $v^*(f) = k$ and p prime in $\mathbb{Z}/p^n\mathbb{Z}[x]$ then irreducible in $\mathbb{Z}/p^n\mathbb{Z}$. □

4.2 Non-zerodivisors to monic polynomials

Proposition 4.3 : *Let R be a commutative ring. The units of $R[x]$ are precisely the polynomials $a_0 + a_1x + ... + a_nx^n$ with a_0 a unit of R and a_l nilpotent for all $l > 0$.*

Proof: Let us consider $f = a_0 + a_1x + ... + a_nx^n$ and P prime ideal, then its image under projection to $(R/P)[x]$ is an unit. Since P is prime (R/P) is an integral domain, and $U((R/P)[x]) = U(R/P)$, therefore a_0 is not in any P and hence an unit, and for $l > 0$, a_l is in every P and therefore nilpotent. Conversely, if $f = a_0 + h$ with a_0 an unit of R and all coeficients of h nilpotent (in the intersection of all prime ideals of R) then h is in every prime ideal of $R[x]$ and hence $f = a_0 + h$ is in no prime ideal of $R[x]$ and then an unit of $R[x]$. □

Corollary 4.4 : *The units of $\mathbb{Z}/p^n\mathbb{Z}[x]$ are precisely the polynomials $f = a_0 + a_1x + ... + a_nx^n$ such that (in $\mathbb{Z}/p^n\mathbb{Z}$) $p \nmid a_0$ and $p \mid a_l$ for all $l > 0$. Then a polynomial in $\mathbb{Z}[x]$ is a unit in $\mathbb{Z}/p^n\mathbb{Z}[x]$ for some $n \geqslant 1$ if and only if is a unit in $\mathbb{Z}/p^n\mathbb{Z}[x]$ for all n.*

Proof: By **Proposition 3.7** and **Proposition 4.3**. a_0 is an unit in $\mathbb{Z}/p^n\mathbb{Z}[x]$ then not a zero-divisor and $v^*(a_0) = 0$ and $p \nmid a_0$. For $l > 0$ a_l is nilpotent then $v^*(a_l) > 0$ and $p \mid a_l$ □

Theorem 4.5 : *If f is a non-zerodivisor, then f is uniquely representable as $f = uh$ with $u \in \mathbb{Z}/p^n\mathbb{Z}[x]$ an unit and h monic with $deg(h) = deg(\overline{f})$ where $\overline{f}$ is the image of f under the canonical projection* Π.

Proof: (Uniqueness only) Suppose that $f = uh = vg$ with $u, v \in \mathbb{Z}/p^n\mathbb{Z}[x]$ units and h, g monic. Then $v^{-1}uh = g$. As h, g are monic, so is $v^{-1}u$. Knowing that the only monic unit in $\mathbb{Z}/p^n\mathbb{Z}[x]$ is 1, we obtain that $u = v$ and $g = h$. □

Proposition 4.6 : *Let $f \in \mathbb{Z}/p^n\mathbb{Z}[x]$, not a zero-divisor. For every factorisation of f $f = c_1...c_k$ into irreducibles, there exists uniquely determined monic irreducible $d_1, ..., d_k \in \mathbb{Z}/p^n\mathbb{Z}[x]$ and units $v_1, ..., v_k \in \mathbb{Z}/p^n\mathbb{Z}[x]$ with $c_i = v_id_i$.*

Proof: Since f is a non-zerodivisor, c_i is a non-zerodivisor $\forall i \in \{1....k\}$. Then by the **Theorem 4.5**, we have unique unit and monic polynomial v_i and d_i such that $c_i = v_id_i$, then $f = c_1....c_k = v_1d_1...v_kd_k = (v_1...v_k).d_1...d_k$ (with $v_1...v_k$ a unit) □

Remark 4.7 : *By the **Theorem 4.5** and **Corollary 4.4** we conclude that (u, h) is uniquely determined by $h = d_1....d_k$ and $u = c_1....c_k$.*
Every non-zero divisor has then only finetely many factorisations into irreducibles (up to associates).

4.3 Monic polynomials to primary monic polynomials

Definition 4.8 : Let R be a commutative ring, and I an ideal of R. We define the radical of I, the ideal such that an element x is in the racidal if some power of x is in I. We denote it by $Rac(I)$

Definiton 4.9 : Let I be a proper ideal of $\mathbb{Z}/p^n\mathbb{Z}[x]$, I is said to be primary if whenever $xy \in I$ then $x \in I$ or for some a natural number $t > 0$ $y^t \in I$.

Definition 4.10 : We call a non-zerodivisor of $\mathbb{Z}/p^n\mathbb{Z}[x]$ primary if its image under projection to $\mathbb{Z}/p\mathbb{Z}[x]$ is associated to a power of an irreducible polynomial.

Proposition 4.11: *An ideal of $\mathbb{Z}/p^n\mathbb{Z}[x]$ that does not consist only of zero-divisors is primary if and only if its radical is a maximal ideal.*

Proof: $\Rightarrow$ Let us take I a primary ideal of $\mathbb{Z}/p^n\mathbb{Z}[x]$. Let us consider $f_1 f_2 \in Rac(I)$ then $\exists t \in \mathbb{N}$ such that $(f_1 f_2)^t = f_1^t f_2^t \in I$ since I is primary $f_1^t \in I$ or $f_2^{tk} \in I$ then $f_1 \in Rac(I)$ or $f_2 \in Rac(I)$ then $Rac(I)$ is prime.
$\Leftarrow$ Let us consider an ideal I such that $Rac(I)$ is maximal. We have $I \subseteq Rac(I)$, since $Rac(I)$ is maximal, $Rac(I)$ prime then I is prime (in particular primary) and $(p) = Z(\mathbb{Z}/p^n\mathbb{Z}[x]) \subsetneq I$, then I is primary and does not consist only of zero-divisors. □

Lemma 4.12 : *Let $f \in \mathbb{Z}/p^n\mathbb{Z}[x]$, not a zero-divisor. Then (f) is a primary ideal of $\mathbb{Z}/p^n\mathbb{Z}[x]$ if and only if the image of f under the canonical projection Π is associated to a power of an irreducible polynomial in $\mathbb{Z}/p\mathbb{Z}[x]$.*

Proof: In the PID $\mathbb{Z}/p\mathbb{Z}[x]$, the non-trivial primary ideals are precisely the principal ideals generated by powers of irreducible elements. We note that the projection Π induces a bijection between primary ideals of $\mathbb{Z}/p\mathbb{Z}[x]$ and primary ideals of $\mathbb{Z}/p^n\mathbb{Z}[x]$ containing (p), then if the image $\overline{f}$ of f under Π is associated to a power of an irreducible polynomial in $\mathbb{Z}/p\mathbb{Z}[x]$, the image $\overline{f}$ belongs to a primary ideal I, then $(\overline{f})$ is also primary and then (f) which contains (p) is primary in $\mathbb{Z}/p^n\mathbb{Z}[x]$. Conversely, we know by **Proposition 4.11** that the radical of (f) is maximal (in particular prime), by using the fact that every prime ideal of $\mathbb{Z}/p^n\mathbb{Z}[x]$ contains (p). We have $(p) \subseteq Rac((f))$ hence $Rac((f)) = Rac((f) + (p))$. But $(f) + (p) = \Pi^{-1}(\Pi((f)))$ therefore, for a non-zerodivisor f, (f) is primary if and only if $Rac(f)$ is maximal which is equivalent to $(f) + (p)$ being primary which is equivalent to $\Pi(f)$ being a primary element of $\mathbb{Z}/p\mathbb{Z}[x]$. □

Theorem 4.13 : *(Hensel's Lemma) Every monic $f \in \mathbb{Z}/p^n\mathbb{Z}[x]$ is a product of primary polynomials. Furthermore, the monic primary factors of a monic polynomial in $\mathbb{Z}/p^n\mathbb{Z}[x]$ are uniquely determined.*

Theorem 4.14 : *Let $f \in \mathbb{Z}/p^n\mathbb{Z}[x]$ monic, then there exist monic polynomials $f_1, ..., f_r \in \mathbb{Z}/p^n\mathbb{Z}[x]$ such that $f = f_1....f_r$ and the residue class of f_i in $\mathbb{Z}/p\mathbb{Z}[x]$ is a power of a monic irreducible polynomial $g_i \in \mathbb{Z}/p\mathbb{Z}[x]$ with $g_1....g_r$ distinct. The polynomials $f_1....f_r \in \mathbb{Z}/p^n\mathbb{Z}[x]$ are primary and uniquely determined (up to ordering).*

(Proof omitted)

5 Non-unique factorization over $\mathbb{Z}/p^n\mathbb{Z}[x]$

Proposition 5.1 : *Every non-zero polynomial $f \in \mathbb{Z}/p^n\mathbb{Z}[x]$ is representable as :*

$$f = p^k u f_1.....f_r$$

with $0 \leqslant k < n$, u a unit of $\mathbb{Z}/p^n\mathbb{Z}[x]$, $r \geqslant 0$, and $f_1, ..., f_r \in \mathbb{Z}/p^n\mathbb{Z}[x]$ monic polynomials such that the residue class of f_i in $\mathbb{Z}/p\mathbb{Z}[x]$ is a power of a monic irreducible polynomial $g_i \in \mathbb{Z}/p\mathbb{Z}[x]$ and $g_1, ..., g_r$ are distinct. Moreover, $k \in \mathbb{N}$ is unique, u is unique modulo $p^{n-k}\mathbb{Z}/p^n\mathbb{Z}[x]$ and also f_i are unique (up to ordering) modulo $p^{n-k}\mathbb{Z}/p^n\mathbb{Z}[x]$.

Proof: Follows directly from: **4.2, 4.6, 4.14**. □

Theorem 5.2 : *Let M' be the submonoid of M consisting of all monic polynomials of $\mathbb{Z}/p^n\mathbb{Z}[x]$ and U its group of units. Then:*

$$M \simeq U \bigoplus M'$$

Furthermore: $M' \simeq \sum_f M_f$ *where f ranges through all monic irreducible polynomials of* $\mathbb{Z}/p\mathbb{Z}[x]$.

Proof: Follows directly from previous statements of uniqueness of factorization into unit and monic primary polynomials. □

Corollary 5.3 : The elasticity of M' is infinite and $\Phi_2(M') = \infty$. Therefore the elasticity of M is infinite as well.

Proof: We proved in the **Theorem 2.7** that the elasticity of each M_f is infinite, then M' as an infinite direct sum of monoids M_f has an infinite elasticity and satisfies $\Phi_2(M') = \infty$. Moreover M is full elastic also. □

6 Algorithm on sage and some examples

6.1 The algorithm

We aim at computing the factorizations of a monic polynomial P in $\mathbb{Z}/p^n\mathbb{Z}[X]$.
As we expect, the inputs should be the polynomial P, a prime p and a positive integer n. The algorithm starts by computing the factorization of P modulo p, which is unique since $\mathbb{Z}/p\mathbb{Z}[x]$ is a UFD.
Then we need to define a function (called "$factor$") to compute the factorizations of upper degrees. The algortihm proceeds as follows:
After computing the factorization of P into irreducible factors in the field $\mathbb{Z}/p\mathbb{Z}[x]$, we use the function $factor(.,.)$ n-1 consecutive times.
This function gets a list and returns an other list. The function considers each element of the input list (namely a factorization), builds $m = deg(P)$ variables (called $t_0, t_1..., t_{m-1} \in \mathbb{Z}/p\mathbb{Z}$) and constructs a list L with all the coefficients $a_i \geqslant 0$ of each factor of the considered factorization (except for the higher degree). For instance, if we work on factorizations in $\mathbb{Z}/p^r\mathbb{Z}$ with $0 < r \leqslant n$, we change all the coefficients a_i of L into $a_i + t_i * p^r$ and reconstruct the factors with these new coefficients, according to the corresponding degrees. Then we expand the product of the new factors, we subtract P and get a polynomial function l of which each coefficient is divisible by p^r. This constitute a system of modular equations that we solve by using "$solve - mod$".
We can divide l by p^r, then each of its coefficients has to equal 0 modulo p, this allows easier calculations.
Afterwards we reconstruct all the new factorizations by replacing all the t_i by their corresponding solution given by $solve - mod$, and get the factorizations of P in $\mathbb{Z}/p^{r+1}\mathbb{Z}$.

The algorithm is this:

```
R.<x>=ZZ[x];                                                        #Inputs
p=2
n=16
#P=x^6+2*x+1
P=x^3+2*x^2+x
#P=x^2

if P.is_irreducible()==true:                                      #Work on reducible polynomials
    print P, 'is irreducible'


else:
    print 'P =',P
    K=P.factor_mod(p)                                             #Factorization mod p
    print 'Factorization of P mod',p,':', K;
    O=[]                                   #List which will contain all the factorizations of P for a certain p^z
    O.append(K)


    def factor(O,z):                #Def a function that compute the factorizations mod p^(z+1), from the previous ones in O
        N=[]
        for y in range(len(O)):
            F=ZZ[x](O[y].expand())
            Vect=[var('t%s' % i) for i in range(F.degree())]           #List of deg(P) variables ti (all factors are monic)
            r=0
            g=1
            for i in range(len(O[y])):                                 #Consider each facotization
                k=O[y][i][0]
                L=[0..k.degree()-1]                                    #List which will contain all new coeffs
                for v in range(O[y][i][1]):                            #Consider each factor
                    S=0
                    H=Vect[r:r+len(L)]
                    for j in range(len(L)):
                              L[j]=ZZ(k[j])+H[j]*p^z
                              S=S+L[j]*x^j
                    r=r+len(L)
                    f(x)=S+x^(k.degree())                               #each coeff ai becomes: ai+ti*p^z
                    g=g*f                                               #re-construction of each facorization


            l=(g.expand().collect(x)-P(x)).expand().collect(x);
            l=l/p^z                                                     #It allows to solve mod p instead of mod p^(z+1)
            L=[l(0)==0]                           #List containing all the new coeffs
            for i in range(1,F.degree()):         #to get the coeffs from a polynomial function (not recognized as polynomial)
                l(x)=l(x)-l(0)
                l(x)=l(x).factor()
                while l(0)==0:
                    l(x)=(l(x)/x).collect(x)
           L.append(l(0)==0)


        b=solve_mod(L,p)#Resolution
        for s in range(len(b)):              #construction of the factorizations with the new coeffs from the resolution
            G(x)=1
            u=0
            for i in range(len(O[y])):
                   k=O[y][i][0];
                   L=[0..k.degree()-1]
                   for v in range(O[y][i][1]):
                       S=0
                       H=b[s][u:u+len(L)]
                       for j in range(len(L)):
                           L[j]=ZZ(k[j])+ZZ(H[j])*p^z
                           S=S+L[j]*x^j
                       f(x)=S+x^(k.degree())
                       u=u+len(L)
                       G=(G*f)
            N.append(G(x))


    O=[]
    O=O+Set(N).list()                                         #to make sure that each factorization occurs only once
    for i in range(len(O)):
        O[i]=ZZ[x](O[i].expand()).factor()
    return O

E=factor(O,1)
print 'There are', len(E), 'factorization of P mod', p^2
print E

for i in range(2,n):                                                 #To repeat the process for each power of p until p^n
    E=factor(E,i)
    print 'There are', len(E), 'factorizations of P mod', p^(i+1)
    print E                                                          #Output
```

6.2 Some examples

Some examples will here illustrate the previous reasoning. Remark that the algorithm returns only the new factorizations, in moving from $\mathbb{Z}/p^r\mathbb{Z}$ to $\mathbb{Z}/p^{r+1}\mathbb{Z}$.

- $P = x^3 + 2x^2 + x$, $p = 2$, $n = 10$

```
P = x^3 + 2*x^2 + x
Factorization of P mod 2 : x * (x + 1)^2
There are 2 factorization of P mod 4
[x * (x + 1)^2, x * (x + 3)^2]
There are 2 factorizations of P mod 8
[x * (x + 1)^2, x * (x + 5)^2]
There are 3 factorizations of P mod 16
[x * (x + 1)^2, x * (x + 5) * (x + 13), x * (x + 9)^2]
There are 3 factorizations of P mod 32
[x * (x + 1)^2, x * (x + 9) * (x + 25), x * (x + 17)^2]
There are 5 factorizations of P mod 64
[x * (x + 33)^2, x * (x + 1)^2, x * (x + 9) * (x + 57), x * (x + 25) *
(x + 41), x * (x + 17) * (x + 49)]
There are 5 factorizations of P mod 128
[x * (x + 1)^2, x * (x + 65)^2, x * (x + 17) * (x + 113), x * (x + 49) *
(x + 81), x * (x + 33) * (x + 97)]
There are 9 factorizations of P mod 256
[x * (x + 1)^2, x * (x + 129)^2, x * (x + 81) * (x + 177), x * (x + 113)
* (x + 145), x * (x + 65) * (x + 193), x * (x + 97) * (x + 161), x * (x
+ 33) * (x + 225), x * (x + 49) * (x + 209), x * (x + 17) * (x + 241)]
There are 9 factorizations of P mod 512
[x * (x + 1)^2, x * (x + 257)^2, x * (x + 65) * (x + 449), x * (x + 129)
* (x + 385), x * (x + 33) * (x + 481), x * (x + 193) * (x + 321), x * (x
+ 161) * (x + 353), x * (x + 225) * (x + 289), x * (x + 97) * (x + 417)]
There are 17 factorizations of P mod 1024
[x * (x + 513)^2, x * (x + 449) * (x + 577), x * (x + 481) * (x + 545),
x * (x + 97) * (x + 929), x * (x + 161) * (x + 865), x * (x + 385) * (x
+ 641), x * (x + 129) * (x + 897), x * (x + 193) * (x + 833), x * (x +
225) * (x + 801), x * (x + 65) * (x + 961), x * (x + 1)^2, x * (x + 33)
* (x + 993), x * (x + 321) * (x + 705), x * (x + 353) * (x + 673), x *
(x + 289) * (x + 737), x * (x + 257) * (x + 769), x * (x + 417) * (x +
609)]
```

- $P = x^3 + 2x^2 + x$, $p = 7$, $n = 5$

```
P = x^3 + 2*x^2 + x
Factorization of P mod 7 : x * (x + 1)^2
There are 4 factorization of P mod 49
[x * (x + 22) * (x + 29), x * (x + 15) * (x + 36), x * (x + 8) * (x +
43), x * (x + 1)^2]
There are 4 factorizations of P mod 343
[x * (x + 148) * (x + 197), x * (x + 50) * (x + 295), x * (x + 99) * (x
+ 246), x * (x + 1)^2]
There are 25 factorizations of P mod 2401
[x * (x + 50) * (x + 2353), x * (x + 834) * (x + 1569), x * (x + 197) *
(x + 2206), x * (x + 687) * (x + 1716), x * (x + 785) * (x + 1618), x *
(x + 99) * (x + 2304), x * (x + 589) * (x + 1814), x * (x + 736) * (x +
1667), x * (x + 1)^2, x * (x + 883) * (x + 1520), x * (x + 344) * (x +
2059), x * (x + 295) * (x + 2108), x * (x + 442) * (x + 1961), x * (x +
393) * (x + 2010), x * (x + 1128) * (x + 1275), x * (x + 638) * (x +
1765), x * (x + 1030) * (x + 1373), x * (x + 1079) * (x + 1324), x * (x
+ 246) * (x + 2157), x * (x + 981) * (x + 1422), x * (x + 540) * (x +
1863), x * (x + 1177) * (x + 1226), x * (x + 491) * (x + 1912), x * (x +
148) * (x + 2255), x * (x + 932) * (x + 1471)]
There are 25 factorizations of P mod 16807
[x * (x + 6861) * (x + 9948), x * (x + 1)^2, x * (x + 5146) * (x +
11663), x * (x + 2059) * (x + 14750), x * (x + 1373) * (x + 15436), x *
(x + 4460) * (x + 12349), x * (x + 5489) * (x + 11320), x * (x + 7204) *
(x + 9605), x * (x + 6518) * (x + 10291), x * (x + 3431) * (x + 13378),
x * (x + 6175) * (x + 10634), x * (x + 3088) * (x + 13721), x * (x +
4117) * (x + 12692), x * (x + 2402) * (x + 14407), x * (x + 7890) * (x +
8919), x * (x + 1030) * (x + 15779), x * (x + 4803) * (x + 12006), x *
(x + 8233) * (x + 8576), x * (x + 1716) * (x + 15093), x * (x + 2745) *
(x + 14064), x * (x + 5832) * (x + 10977), x * (x + 3774) * (x + 13035),
x * (x + 687) * (x + 16122), x * (x + 7547) * (x + 9262), x * (x + 344)
* (x + 16465)]
```

- $P = x^7 - 15x^4 + 2x^3 - 8x^2 - 16x$, $p = 2$, $n = 4$

```
P = x^7 - 15*x^4 + 2*x^3 - 8*x^2 - 16*x
Factorization of P mod 2 : (x + 1) * x^4 * (x^2 + x + 1)
There are 2 factorization of P mod 4
[(x + 2) * (x + 3) * x^3 * (x^2 + 3*x + 3), x * (x + 3) * (x + 2)^3 *
(x^2 + 3*x + 3)]
There are 4 factorizations of P mod 8
[(x + 2) * (x + 3) * x^3 * (x^2 + 3*x + 3), (x + 3) * (x + 4) * (x + 6)
* x^2 * (x^2 + 3*x + 3), x * (x + 2) * (x + 3) * (x + 4)^2 * (x^2 + 3*x
+ 3), (x + 3) * (x + 6) * (x + 4)^3 * (x^2 + 3*x + 3)]
There are 10 factorizations of P mod 16
[(x + 6) * (x + 11) * (x + 12) * (x + 8)^2 * (x^2 + 3*x + 11), (x + 6) *
(x + 11) * (x + 4)^3 * (x^2 + 3*x + 11), (x + 11) * (x + 14) * (x +
12)^3 * (x^2 + 3*x + 11), (x + 4) * (x + 11) * (x + 14) * (x + 8)^2 *
(x^2 + 3*x + 11), (x + 4) * (x + 11) * (x + 14) * x^2 * (x^2 + 3*x +
11), (x + 4) * (x + 6) * (x + 11) * (x + 12)^2 * (x^2 + 3*x + 11), (x +
11) * (x + 12) * (x + 14) * (x + 4)^2 * (x^2 + 3*x + 11), (x + 6) * (x +
11) * (x + 12) * x^2 * (x^2 + 3*x + 11), x * (x + 4) * (x + 6) * (x + 8)
* (x + 11) * (x^2 + 3*x + 11), x * (x + 8) * (x + 11) * (x + 12) * (x +
14) * (x^2 + 3*x + 11)]
```

- $P = x^2 + 2x + 1$, $p = 5$, $n = 4$

```
P = x^2 + 2*x + 1
Factorization of P mod 5 : (x + 1)^2
There are 3 factorization of P mod 25
[(x + 6) * (x + 21), (x + 11) * (x + 16), (x + 1)^2]
There are 3 factorizations of P mod 125
[(x + 26) * (x + 101), (x + 51) * (x + 76), (x + 1)^2]
There are 13 factorizations of P mod 625
[(x + 301) * (x + 326), (x + 101) * (x + 526), (x + 26) * (x + 601), (x
+ 151) * (x + 476), (x + 76) * (x + 551), (x + 1)^2, (x + 201) * (x +
426), (x + 251) * (x + 376), (x + 126) * (x + 501), (x + 51) * (x +
576), (x + 276) * (x + 351), (x + 226) * (x + 401), (x + 176) * (x +
451)]
There are 13 factorizations of P mod 3125
[(x + 1001) * (x + 2126), (x + 1126) * (x + 2001), (x + 376) * (x +
2751), (x + 1)^2, (x + 501) * (x + 2626), (x + 251) * (x + 2876), (x +
126) * (x + 3001), (x + 751) * (x + 2376), (x + 1376) * (x + 1751), (x +
1501) * (x + 1626), (x + 626) * (x + 2501), (x + 1251) * (x + 1876), (x
+ 876) * (x + 2251)]
There are 63 factorizations of P mod 15625
[(x + 7126) * (x + 8501), (x + 7001) * (x + 8626), (x + 4376) * (x +
11251), (x + 1751) * (x + 13876), (x + 1626) * (x + 14001), (x + 4501) *
(x + 11126), (x + 1876) * (x + 13751), (x + 4251) * (x + 11376), (x +
2126) * (x + 13501), (x + 4001) * (x + 11626), (x + 1376) * (x + 14251),
(x + 4751) * (x + 10876), (x + 6626) * (x + 9001), (x + 4876) * (x +
10751), (x + 1251) * (x + 14376), (x + 1126) * (x + 14501), (x + 126) *
(x + 15501), (x + 1001) * (x + 14626), (x + 6376) * (x + 9251), (x +
3751) * (x + 11876), (x + 1)^2, (x + 3626) * (x + 12001), (x + 6501) *
(x + 9126), (x + 3876) * (x + 11751), (x + 6251) * (x + 9376), (x +
7501) * (x + 8126), (x + 2001) * (x + 13626), (x + 7376) * (x + 8251),
(x + 2751) * (x + 12876), (x + 4626) * (x + 11001), (x + 5501) * (x +
10126), (x + 2876) * (x + 12751), (x + 7251) * (x + 8376), (x + 3126) *
(x + 12501), (x + 3001) * (x + 12626), (x + 376) * (x + 15251), (x +
5751) * (x + 9876), (x + 5626) * (x + 10001), (x + 501) * (x + 15126),
(x + 5876) * (x + 9751), (x + 251) * (x + 15376), (x + 6126) * (x +
9501), (x + 7626) * (x + 8001), (x + 5376) * (x + 10251), (x + 751) * (x
```

(We cannot display the whole output)

- $P = x^2 + 2x + 1$, $p = 13$, $n = 4$

```
P = x^2 + 2*x + 1
Factorization of P mod 13 : (x + 1)^2
There are 7 factorization of P mod 169
[(x + 53) * (x + 118), (x + 27) * (x + 144), (x + 1)^2, (x + 66) * (x +
105), (x + 14) * (x + 157), (x + 79) * (x + 92), (x + 40) * (x + 131)]
There are 7 factorizations of P mod 2197
[(x + 846) * (x + 1353), (x + 1015) * (x + 1184), (x + 1)^2, (x + 170) *
(x + 2029), (x + 677) * (x + 1522), (x + 508) * (x + 1691), (x + 339) *
(x + 1860)]
There are 85 factorizations of P mod 28561
[(x + 4902) * (x + 23661), (x + 9127) * (x + 19436), (x + 170) * (x +
28393), (x + 677) * (x + 27886), (x + 4395) * (x + 24168), (x + 14197) *
(x + 14366), (x + 8113) * (x + 20450), (x + 3888) * (x + 24675), (x +
10141) * (x + 18422), (x + 5916) * (x + 22647), (x + 2198) * (x +
26365), (x + 13690) * (x + 14873), (x + 10648) * (x + 17915), (x + 6423)
* (x + 22140), (x + 1)^2, (x + 13183) * (x + 15380), (x + 1691) * (x +
26872), (x + 10817) * (x + 17746), (x + 6592) * (x + 21971), (x + 13521)
* (x + 15042), (x + 8620) * (x + 19943), (x + 10310) * (x + 18253), (x +
1353) * (x + 27210), (x + 14028) * (x + 14535), (x + 5578) * (x +
22985), (x + 6085) * (x + 22478), (x + 1860) * (x + 26703), (x + 9803) *
(x + 18760), (x + 8958) * (x + 19605), (x + 9296) * (x + 19267), (x +
4733) * (x + 23830), (x + 508) * (x + 28055), (x + 339) * (x + 28224),
(x + 9465) * (x + 19098), (x + 5240) * (x + 23323), (x + 1015) * (x +
27548), (x + 9972) * (x + 18591), (x + 846) * (x + 27717), (x + 5409) *
(x + 23154), (x + 1184) * (x + 27379), (x + 5071) * (x + 23492), (x +
9634) * (x + 18929), (x + 12845) * (x + 15718), (x + 6761) * (x +
21802), (x + 2536) * (x + 26027), (x + 10986) * (x + 17577), (x + 11493)
* (x + 17070), (x + 7268) * (x + 21295), (x + 13352) * (x + 15211), (x +
3550) * (x + 25013), (x + 13859) * (x + 14704), (x + 7775) * (x +
20788), (x + 1522) * (x + 27041), (x + 5747) * (x + 22816), (x + 4057) *
(x + 24506), (x + 8282) * (x + 20281), (x + 8789) * (x + 19774), (x +
4564) * (x + 23999), (x + 6254) * (x + 22309), (x + 10479) * (x +
18084), (x + 4226) * (x + 24337), (x + 2029) * (x + 26534), (x + 8451) *
(x + 20112), (x + 12169) * (x + 16394), (x + 7944) * (x + 20619), (x +
```

- $P = x^6 + x^5 - x^4 + 2x^3 + 11x^2 - 12x$, $p = 3$, $n = 8$

```
P = x^6 + x^5 - x^4 + 2*x^3 + 11*x^2 - 12*x
Factorization of P mod 3 : x^2 * (x^4 + x^3 + 2*x^2 + 2*x + 2)
There are 2 factorization of P mod 9
[(x + 6)^2 * (x^4 + 7*x^3 + 5*x^2 + 5*x + 5), x * (x + 3) * (x^4 + 7*x^3
+ 5*x^2 + 5*x + 5)]
There are 3 factorizations of P mod 27
[(x + 12) * (x + 18) * (x^4 + 25*x^3 + 5*x^2 + 14*x + 23), (x + 9) * (x
+ 21) * (x^4 + 25*x^3 + 5*x^2 + 14*x + 23), x * (x + 3) * (x^4 + 25*x^3
+ 5*x^2 + 14*x + 23)]
There are 3 factorizations of P mod 81
[(x + 30) * (x + 54) * (x^4 + 79*x^3 + 5*x^2 + 68*x + 50), x * (x + 3) *
(x^4 + 79*x^3 + 5*x^2 + 68*x + 50), (x + 27) * (x + 57) * (x^4 + 79*x^3
+ 5*x^2 + 68*x + 50)]
There are 3 factorizations of P mod 243
[x * (x + 165) * (x^4 + 79*x^3 + 86*x^2 + 149*x + 212), (x + 3) * (x +
162) * (x^4 + 79*x^3 + 86*x^2 + 149*x + 212), (x + 81) * (x + 84) * (x^4
+ 79*x^3 + 86*x^2 + 149*x + 212)]
There are 3 factorizations of P mod 729
[(x + 408) * (x + 486) * (x^4 + 565*x^3 + 86*x^2 + 392*x + 212), x * (x
+ 165) * (x^4 + 565*x^3 + 86*x^2 + 392*x + 212), (x + 243) * (x + 651) *
(x^4 + 565*x^3 + 86*x^2 + 392*x + 212)]
There are 3 factorizations of P mod 2187
[(x + 894) * (x + 1458) * (x^4 + 2023*x^3 + 815*x^2 + 1121*x + 941), (x
+ 729) * (x + 1623) * (x^4 + 2023*x^3 + 815*x^2 + 1121*x + 941), x * (x
+ 165) * (x^4 + 2023*x^3 + 815*x^2 + 1121*x + 941)]
There are 3 factorizations of P mod 6561
[(x + 2187) * (x + 2352) * (x^4 + 2023*x^3 + 3002*x^2 + 1121*x + 3128),
x * (x + 4539) * (x^4 + 2023*x^3 + 3002*x^2 + 1121*x + 3128), (x + 165)
* (x + 4374) * (x^4 + 2023*x^3 + 3002*x^2 + 1121*x + 3128)]
```

- $P = x^6 + x^5 - x^4 + 2x^3 + 11x^2 - 12x$, $p = 2$, $n = 8$

```
P = x^6 + x^5 - x^4 + 2*x^3 + 11*x^2 - 12*x
Factorization of P mod 2 : (x + 1) * x^2 * (x^3 + x + 1)
There are 2 factorization of P mod 4
[(x + 1) * (x + 2)^2 * (x^3 + 3*x + 3), (x + 1) * x^2 * (x^3 + 3*x + 3)]
There are 1 factorizations of P mod 8
[x * (x + 4) * (x + 5) * (x^3 + 3*x + 7)]
There are 2 factorizations of P mod 16
[x * (x + 12) * (x + 13) * (x^3 + 8*x^2 + 11*x + 15), (x + 4) * (x + 8)
* (x + 13) * (x^3 + 8*x^2 + 11*x + 15)]
There are 4 factorizations of P mod 32
[x * (x + 13) * (x + 28) * (x^3 + 24*x^2 + 27*x + 15), (x + 12) * (x +
13) * (x + 16) * (x^3 + 24*x^2 + 27*x + 15), (x + 8) * (x + 13) * (x +
20) * (x^3 + 24*x^2 + 27*x + 15), (x + 4) * (x + 13) * (x + 24) * (x^3 +
24*x^2 + 27*x + 15)]
There are 4 factorizations of P mod 64
[(x + 13) * (x + 28) * (x + 32) * (x^3 + 56*x^2 + 59*x + 15), x * (x +
13) * (x + 60) * (x^3 + 56*x^2 + 59*x + 15), (x + 12) * (x + 13) * (x +
48) * (x^3 + 56*x^2 + 59*x + 15), (x + 13) * (x + 16) * (x + 44) * (x^3
+ 56*x^2 + 59*x + 15)]
There are 4 factorizations of P mod 128
[(x + 13) * (x + 28) * (x + 96) * (x^3 + 120*x^2 + 123*x + 15), (x + 13)
* (x + 60) * (x + 64) * (x^3 + 120*x^2 + 123*x + 15), (x + 13) * (x +
32) * (x + 92) * (x^3 + 120*x^2 + 123*x + 15), x * (x + 13) * (x + 124)
* (x^3 + 120*x^2 + 123*x + 15)]
There are 4 factorizations of P mod 256
[(x + 60) * (x + 141) * (x + 192) * (x^3 + 120*x^2 + 251*x + 15), (x +
64) * (x + 141) * (x + 188) * (x^3 + 120*x^2 + 251*x + 15), (x + 124) *
(x + 128) * (x + 141) * (x^3 + 120*x^2 + 251*x + 15), x * (x + 141) * (x
+ 252) * (x^3 + 120*x^2 + 251*x + 15)]
```

7 References

[1] *Frei/Frisch : Non-unique factorization of polynomial over residue class rings of the integers. Commutative Algebra 39 (2011), no.4, 1482-1490.*

[2] *A.G A$\overline{G}$*ARGÜN, *D.D. ANDERSON, AND VALDES-LEON, Factorisation in commutative rings with zero-divisors. III., Rocky Mountain J.Math.31 (2001), 1-21.*

[3] *D.D ANDERSON AND S.VALDES − LEON*, *Factorisation in commutative rings with zero divisors, Rocky Mountain J.Math.26 (1996), 439-480.*

[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, 1997, 197-219.*

[5] *J.J JIANG*, *G.H PENG*, *On polynomial functions over finite commutative rings, Acta Math. Sin.(Engl.Ser.) 22 (2006), 1047-1050.*

[6] *PAUL ZIMMERMANN*, *Calcul mathémathique avec Sage (Sagebook).*

8 Acknowledgement

The author wishes to thank Pr.WIESE and Dr.TSAKNIAS for providing valuable advice on this subject.