Available online at www.sciencedirect.com

SCIENCE DIRECT®

Finite Fields and Their Applications 11 (2005) 56–70

FINITE FIELDS AND THEIR APPLICATIONS

http://www.elsevier.com/locate/ffa

Factoring polynomials over $\mathbb{Z}_4$ and over certain Galois rings

Ana Sălăgean*

Department of Computer Science, Loughborough University, Loughborough LE11 3TU, UK

Received 2 September 2003; revised 7 May 2004

Communicated by Igor Shparlinski

Abstract

It is known that univariate polynomials over finite local rings factor uniquely into primary pairwise coprime factors. Primary polynomials are not necessarily irreducible. Here we describe a factorisation into irreducible factors for primary polynomials over $\mathbb{Z}_4$ and more generally over Galois rings of characteristic p^2. An algorithm is also given. As an application, we factor $x^n - 1$ and $x^n + 1$ over such rings.

Keywords: Polynomial factoring; Galois rings; Cyclic codes over rings

1. Introduction

Univariate polynomials over a finite local ring factor uniquely into primary pairwise coprime factors (see [9]). A primary polynomial might be irreducible (for example $x^2 + 2$ is irreducible in $\mathbb{Z}_4[x]$) or reducible, in which case its factorisation will in general not be unique (for example $x^2 = (x + 2)^2$ in $\mathbb{Z}_4[x]$). Not even the number of factors and their degrees are unique (for example $x^4 = (x^2 + 2)^2$ in $\mathbb{Z}_4[x]$).

We describe a factorisation of primary polynomials into irreducible factors over a Galois ring of characteristic p^2 (p being a prime), giving also an algorithm. The

* Fax: +44-1509-211-586.

E-mail address: a.m.salagean@lboro.ac.uk.

1071-5797/$ - see front matter
doi:10.1016/j.ffa.2004.05.001

factorisation we obtain has the property that it has the maximum number of irreducible factors; moreover, among all factorisation into the maximum number of irreducible factors, it has the minimal number of distinct factors (this number will turn out to be always one or two). We also describe all the factorisations into the maximum number of irreducible factors.

Our interest in polynomials over $\mathbb{Z}_4$, and more generally, Galois rings was motivated by the existence of good error-correcting codes over $\mathbb{Z}_4$ and over Galois rings [8]. Cyclic codes of length n over a ring R are ideals in $R[x]/\langle x^n-1\rangle$. So the factorisation of x^n-1 is particularly important for this application. Another closely related motivation comes from sequences over $\mathbb{Z}_4$ and over Galois rings. Here again polynomials of the form x^n-1 play an important role. As all recurrent sequences are periodic, they are in particular linearly recurrent and satisfy the linear recurrence (of not necessarily minimal degree) defined by x^n-1, with n the period of the sequence.

An algorithm for determining all factorisations of a polynomial over a ring of the form $\mathbb{Z}_{p^a}$ (and some other types of rings) was developed in [13]. One factorisation is derived from the factorisation of the polynomial over the p-adic integers (this can be obtained by the algorithms of Chistov, Ford–Zassenhaus, Buchmann–Lenstra, Cantor–Gordon, Pauli, Ford et al. see [2,4,5,6,7,10]). However, this approach only works when the discriminant of the polynomial (as a p-adic number) is not a multiple of p^a. (For example, it cannot be directly applied to factoring x^n-1 over $\mathbb{Z}_4$ when n is even.) Factoring over the p-adics and then projecting the factorisation to $\mathbb{Z}_{p^a}[x]$ does not always result in a factorisation into irreducible factors, as irreducible monic polynomials over the p-adic integers may no longer be irreducible when projected (see Example 4.6 for illustration).

The advantage of our results compared to [13] is that they hold for all polynomials, regardless of the value of their discriminant. The disadvantage is that they only hold in Galois rings of characteristic p^2, with no immediate way of extending them to Galois rings of characteristic p^a with $a>2$.

The paper is organised as follows. We start by recalling known results in Section 2. Section 3 gives an irreducibility criterion for polynomials over a Galois ring. We then restrict our attention to Galois rings of characteristic p^2 and fully describe in Section 4 factorisations of the primary polynomials in this case. An algorithm will also result. We also note an interesting connection between the factorisation of a polynomial f and $\mathrm{GR}(p^2,r)[x]/\langle f\rangle$ being a principal ideal ring (see Theorem 4.10). In Section 5 we apply our results to factoring x^n-1 and x^n+1 over Galois rings of characteristic p^2 (including $\mathbb{Z}_4$ as an important special case).

2. Preliminaries

Recall that if K is a field, $K[x]$ is a unique factorisation domain. A polynomial is prime if and only if it is irreducible. When K is a finite field there are algorithms for factoring a polynomial into irreducible factors over $K[x]$ (see [1]).

We will recall some known results on the factorisation of polynomials over a finite local ring, following mainly [9].

Let R be a finite local ring and let M be its maximal ideal. All elements of M are nilpotent and all elements of $R \setminus M$ are units. The field $K := R/M$ is called the residue field of R. We denote by $\overline{c}$ the image of $c \in R$ under the canonical projection from R to K. This projection extends naturally to a projection from $R[x]$ to $K[x]$. We will call a polynomial *monic* if its leading coefficient is 1. A polynomial in $R[x]$ is called *regular* if it is not a zero-divisor.

Theorem 2.1 (*[9, Theorems XIII.2 and XIII.6]*). *Let* $f = \sum_{i=0}^{m} c_i x^i \in R[x] \setminus \{0\}$. *Then*:

(i) *f is a zero-divisor iff $c_i \in M$ for $i = 0, \ldots, m$,*
(ii) *f is a unit iff c_0 is a unit and $c_i \in M$ for $i = 1, \ldots, m$,*
(iii) *f is regular iff there is an i, $0 \leqslant i \leqslant m$ such that c_i is a unit,*
(iv) *If f is regular then there are unique polynomials $f^*, u \in R[x]$ such that $f = uf^*$, u is a unit and f^* is monic.*

So based on Theorem 2.1(iv) we can assume that a regular polynomial is monic. Also, when looking at factorisations of a monic polynomial we can assume, without loss of generality, that all factors are monic.

Prime polynomials are irreducible. However, unlike in the case of fields, irreducible polynomials need not be prime. Recall that a polynomial $f \in R[x]$ is called *basic irreducible* if $\overline{f}$ is irreducible in $K[x]$. Obviously, basic irreducible polynomials are irreducible.

A polynomial $f \in R[x]$ is called primary if the ideal $\langle f \rangle$ is primary in $R[x]$, i.e. if for all $gh \in \langle f \rangle$ we have $g \in \langle f \rangle$ or $h^m \in \langle f \rangle$ for some integer $m \geqslant 1$. Primary polynomials in $K[x]$ are powers of prime polynomials. Primary polynomials in $R[x]$ are characterised below:

Theorem 2.2 (*[9, Proposition XIII.12]*). *Let f be a regular non-unit polynomial. The following assertions are equivalent*:

(i) *f is primary,*
(ii) *$\overline{f} = uG^m$ for some unit $u \in K$, $m \geqslant 1$ and $G \in K[x]$ prime,*
(iii) *$f = ug^m + h$ for some $u, g, h \in R[x]$, $m \geqslant 1$ with u unit, g basic irreducible and $h \in M[x]$.*

$R[x]$ is not a unique factorisation domain. However, polynomials in $R[x]$ factor uniquely into primary pairwise coprime factors:

Theorem 2.3 (*[9, Theorem XIII.11]*). *Let $f \in R[x]$ be a regular polynomial. Then $f = uf_1 f_2 \cdots f_s$ with $u \in R[x]$ a unit and $f_1, \ldots, f_s \in R[x]$ regular primary pairwise coprime polynomials. The factors f_i are unique up to multiplication by units.*

The proof of the above theorem is constructive and uses Hensel lifting. We recall here the main steps. By Theorem 2.1(iv) we may assume that f is monic. First we factor $\overline{f}$ in $K[x]$, say $\overline{f} = F_1^{m_1} \ldots F_s^{m_s}$ with $F_i \in K[x]$ irreducible and $m_i \geqslant 1$ for

$i = 1, \ldots, s$. Since $F_i^{m_i}$ are coprime polynomials, one can use Hensel lifting to obtain a factorisation $f = f_1 \cdots f_s$ with $f_i \in R[x]$, $\overline{f_i} = F_i^{m_i}$ and f_i pairwise coprime. By Theorem 2.2, f_i are primary polynomials.

Throughout the paper p will be a prime number and $\mathbb{Z}_{p^a}$ the ring of integers modulo p^a. The Galois field with p^r elements is denoted $\mathrm{GF}(p^r)$. We denote by $\mathrm{GR}(p^a, r)$ the Galois ring obtained as $\mathbb{Z}_{p^a}[y]/\langle f \rangle$ with $f \in \mathbb{Z}_{p^a}[y]$ a monic basic irreducible polynomial of degree r. Note that the characteristic of $\mathrm{GR}(p^a, r)$ is p^a. In this paper we will assume $a \geqslant 2$, so that the Galois ring is not a field.

Note that Galois rings are finite local rings. The maximal ideal of $\mathrm{GR}(p^a, r)$ is $M = \langle p \rangle$ and the residue field is $K = \mathrm{GF}(p^r)$. We have $\overline{c} = c \bmod p$ for all $c \in \mathrm{GR}(p^a, r)$. Every element of $\mathrm{GR}(p^a, r)$ can be uniquely written as up^i with $0 \leqslant i < a$, i uniquely determined and $u \in \mathrm{GR}(p^a, r)$ a unit, unique modulo p^{a-i}. For any $c \in \mathrm{GR}(p^a, r)$ if $p^i c = 0$ then c is divisible by p^{a-i}.

All the previous theorems hold in particular for Galois rings. Theorem 2.2 yields in this case:

Corollary 2.4. *Let $f \in \mathrm{GR}(p^a, r)[x]$ be a monic polynomial. Then f is primary* iff *$f = g^m + ph$ for some $g, h \in \mathrm{GR}(p^a, r)[x]$, $m \geqslant 1$ with g monic and basic irreducible.*

Note that the polynomials g and h in the corollary above are in general not unique.

3. Irreducibility criterion for primary polynomials over Galois rings

We start with a necessary (but not sufficient in general) condition for the reducibility of a primary polynomial over a Galois ring.

Theorem 3.1. *Let $f \in \mathrm{GR}(p^a, r)[x]$ be a monic primary polynomial which is not basic irreducible. Let $g, h \in \mathrm{GR}(p^a, r)[x]$ and $m \geqslant 2$ be such that $f = g^m + ph$ and g is monic basic irreducible. If f factors then $\overline{h} = 0$ or $\overline{g} | \overline{h}$.*

Proof. Since f factors, there are $f_1, f_2 \in \mathrm{GR}(p^a, r)[x]$ monic non-constant polynomials such that $f = f_1 f_2$. Since $\overline{f} = \overline{g}^m = \overline{f_1 f_2}$, we can write $f_i = g^{m_i} + ph_i$ for some $m_i > 0$, $h_i \in \mathrm{GR}(p^a, r)[x]$ for $i = 1, 2$ with $m_1 + m_2 = m$. Without loss of generality we can assume $m_1 \leq m_2$. We have

$$\begin{aligned} f &= (g^{m_1} + ph_1)(g^{m_2} + ph_2) = g^m + pg^{m_1}(h_2 + h_1 g^{m_2 - m_1}) + p^2 h_1 h_2 \\ &= g^m + ph. \end{aligned}$$

Hence $\overline{h} = \overline{g^{m_1}(h_2 + h_1 g^{m_2 - m_1})}$ and therefore we have either $\overline{h} = 0$ or $\overline{g} | \overline{h}$ as required. □

The converse of the above theorem does not hold in general, as the following example shows. However, if the Galois ring is of the form $\mathrm{GR}(p^2, r)$, the converse does hold, see Theorem 4.1.

Example 3.2. Let $f = (x+1)^4 + 4x \in \mathbb{Z}_8[x]$. Putting $g = x+1$ and $h = 2x$ we have $f = g^4 + 2h$ and g is monic basic irreducible. Note that $\overline{h} = 0$. Moreover, any other polynomials g, h such that $f = g^4 + 2h$ and g is monic basic irreducible are of the form $g = x + 1 + 2w$ for some $w \in \mathbb{Z}_8$ and $2h = f - (x+1+2w)^4 = 4x$, and so $\overline{h} = 0$. So f satisfies the conclusion of Theorem 3.1. However, we will show shortly that f is irreducible. So Theorem 3.1 gives a necessary, but not sufficient condition for a polynomial to factor.

We show now that f is irreducible. It can be easily checked that f has no roots in $\mathbb{Z}_8$, so it cannot have any monic factor of degree one. So we are left with the possibility of f factoring into two monic factors of degree two: $f = ((x+1)^2 + 2(Ax+B))((x+1)^2 + 2(Cx+D))$ for some $A, B, C, D \in \mathbb{Z}_8$. By comparing like coefficients of these polynomials we obtain a system of equations in the unknowns A, B, C and D which has no solutions in $\mathbb{Z}_8$.

A sufficient condition for the irreducibility of a polynomial immediately results from Theorem 3.1. It can be viewed as a generalised Eisenstein criterion:

Corollary 3.3. *Let $f \in \mathrm{GR}(p^a, r)[x]$ be a monic primary polynomial which is not basic irreducible. Let $g, h \in \mathrm{GR}(p^a, r)[x]$ and $m \geqslant 2$ be such that $f = g^m + ph$ and g is monic basic irreducible. If $\overline{h} \neq 0$ and $\overline{g} \nmid \overline{h}$ then f is irreducible.*

Example 3.4. A polynomial of the form $f = x^s + p(a_{s-1}x^{s-1} + \cdots + a_0) \in \mathrm{GR}(p^a, r)[x]$ with a_0 a unit is called an Eisenstein polynomial (see for example [9, p. 341]). Putting $g = x$ and $h = a_{s-1}x^{s-1} + \cdots + a_0$, we see that $\overline{h} \neq 0$ and $\overline{g} \nmid \overline{h}$. So by Corollary 3.3, f is irreducible, as expected.

If f is a polynomial such that $\overline{f}$ is square-free, the factorisation of f into primary pairwise coprime factors (given by Theorem 2.3) is a factorisation into basic irreducible factors. If $\overline{f}$ is not square-free, some of the primary factors may factor further. Below we give a sufficient condition for all primary factors in the factorisation given by Theorem 2.3 to be irreducible. Note that checking this condition does not require factoring the polynomial.

Proposition 3.5. *Let $f \in \mathrm{GR}(p^a, r)[x]$ be such that $\overline{f}$ is not square-free. Let f_1, f_2 be any polynomials in $\mathrm{GR}(p^a, r)[x]$ such that $\overline{f_1}$ is the square-free part of $\overline{f}$ and $\overline{f} = \overline{f_1 f_2}$. Let $h \in \mathrm{GR}(p^a, r)[x]$ be such that $ph = f - f_1 f_2$. If $\overline{h} \neq 0$ and $\overline{h}$ and $\overline{f_2}$ are coprime then the factorisation of f into primary pairwise coprime factors (given by Theorem 2.3) is a factorisation into irreducible factors.*

Proof. Let $\overline{f} = \prod_{i=1}^{s} G_i^{m_i}$ be the factorisation of $\overline{f}$ into irreducible polynomials in $\mathrm{GF}(p^r)[x]$. Let g_i be any polynomials such that $\overline{g}_i = G_i$. We have $\overline{f_1} = \prod_{i=1}^{s} G_i$ and $\overline{f_2} = \prod_{i=1}^{s} G_i^{m_i - 1}$, so $f_1 = \prod_{i=1}^{s} g_i + pw_1$ and $f_2 = \prod_{i=1}^{s} g_i^{m_i - 1} + pw_2$ for some $w_1, w_2 \in \mathrm{GR}(p^a, r)[x]$. The factorisation of f given by Theorem 2.3 is of the form $f = \prod_{i=1}^{s}(g_i^{m_i} + ph_i)$ for some $h_i \in \mathrm{GR}(p^a, r)$. To show that this is a factorisation into irreducible factors it suffices (by Corollary 3.3) to show that for any i for which

$m_i > 1$ we have $\overline{h}_i \neq 0$ and $G_i \nmid \overline{h_i}$. By hypothesis, $\overline{h} \neq 0$ and $\overline{h}$ and $\overline{f_2}$ are coprime, so $\overline{h}$ is not divisible by any of the G_i for which $m_i > 1$. Computing $f - f_1 f_2$ we obtain $\overline{h} = \sum_{i=1}^{s} \overline{h}_i \prod_{j \neq i} G_j^{m_j} - \overline{w}_1 \prod_{i=1}^{s} G_i^{m_i - 1} - \overline{w}_2 \prod_{i=1}^{s} G_i$. Fix an i such that $m_i > 1$. In the last equality above, all the terms on the right hand side are divisible by G_i except possibly for $\overline{h}_i \prod_{j \neq i} G_j^{m_j}$. Since the left hand side is not divisible by G_i we deduce $\overline{h}_i \neq 0$ and $G_i \nmid \overline{h_i}$ as required. □

4. Factorisation of primary polynomials over GR(p^2, r)

From this point on, we will restrict the coefficient ring to a Galois ring of characteristic p^2. Theorem 3.1 can be improved in this setting, giving a necessary and sufficient condition for a primary polynomial to factor.

Theorem 4.1. *Let $f \in \mathrm{GR}(p^2, r)[x]$ be a monic primary polynomial which is not basic irreducible. Let $g, h \in \mathrm{GR}(p^2, r)[x]$ and $m \geqslant 2$ be such that $f = g^m + ph$ and g is monic basic irreducible. Then f factors if and only if $\overline{h} = 0$ or $\overline{g} | \overline{h}$.*

Proof. The direct implication follows from Theorem 3.1. We prove the converse. If $\overline{h} = 0$ then $ph = 0$ so $f = g^m$ and this is a factorisation of f into irreducible factors. If $\overline{h} \neq 0$ let $m_1 \geqslant 1$ be maximal such that $\overline{g}^{m_1} | \overline{h}$ and choose w so that $\overline{h} = \overline{g}^{m_1} \overline{w}$. Since $p^2 = 0$, we have $ph = pg^{m_1} w$. We thus obtain the factorisation $f = g^m + ph = g^m + pg^{m_1} w = g^{m_1}(g^{m-m_1} + pw)$. By Corollary 3.3, $g^{m-m_1} + pw$ is irreducible since $\overline{w} \neq 0$ and $\overline{g} \nmid \overline{w}$ by construction. So we factored f into irreducible factors. □

The proof of the above theorem also yields:

Corollary 4.2. *Let $f \in \mathrm{GR}(p^2, r)[x]$ be a monic primary polynomial which is not basic irreducible. The following assertions are equivalent*:

(i) *f factors,*
(ii) *f has a basic irreducible factor,*
(iii) *for all $g \in \mathrm{GR}(p^2, r)[x]$, if g is basic irreducible and $\overline{g} | \overline{f}$ then $g | f$.*

When the Galois ring has characteristic p^2, the converse of Corollary 3.3 also holds:

Corollary 4.3. *Let $f \in \mathrm{GR}(p^2, r)[x]$ be a monic primary polynomial which is not basic irreducible. Let $g, h \in \mathrm{GR}(p^2, r)[x]$ and $m \geqslant 2$ be such that $f = g^m + ph$ and g is monic basic irreducible. Then f is irreducible if and only if $\overline{h} \neq 0$ and $\overline{g} \nmid \overline{h}$.*

If a polynomial in $\mathrm{GR}(p^2, r)$ factors, there are in general several possible factorisations. We will concentrate here on factorisations that are "maximal" in the sense that they contain the maximum number of (not necessarily distinct) factors.

Theorem 4.4. *Let $f \in \mathrm{GR}(p^2, r)[x]$ be a monic primary polynomial which is not irreducible. Let $m \geqslant 2$ and $G \in \mathrm{GF}(p^r)[x]$ be the uniquely determined elements such that $\overline{f} = G^m$ in $\mathrm{GF}(p^r)[x]$. Then f admits a factorisation into monic irreducible factors of one (but not both) of the following two types*:

(i)
$$f = g^m \tag{1}$$

for some $g \in \mathrm{GR}(p^2, r)[x]$ such that g is monic and $\overline{g} = G$.

(ii)
$$f = g^{m_1}(g^{m-m_1} + pw) \tag{2}$$

for some $g, w \in \mathrm{GR}(p^2, r)[x]$ and $1 \leqslant m_1 < m$ such that g is monic, $\overline{g} = G$, $g^{m-m_1} + pw$ is irreducible and if $p \nmid m$ then $m - m_1 \geqslant 2$.

The factorisations given above have the following property: they are factorisations of f into the maximum number of (not necessarily distinct) irreducible factors, and among all possible factorisations into the maximum number of irreducible factors, they consist of a minimum number of distinct factors. Moreover, all factorisations of f into monic irreducible factors having this property are factorisations of type (i) or (ii) and can be obtained as follows: In case (i), if $p \nmid m$ then g is uniquely determined; if $p|m$ then any monic $g \in \mathrm{GR}(p^2, r)[x]$ with $\overline{g} = G$ satisfies (1). In case (ii), m_1 is uniquely determined and for any monic $g \in \mathrm{GR}(p^2, r)[x]$ with $\overline{g} = G$ there is a unique irreducible polynomial of the form $g^{m-m_1} + pw$, with $w \in \mathrm{GR}(p^2, r)[x]$, so that (2) is satisfied.

Proof. The fact that f can be written as in (1) or (2) follows from Theorem 4.1 and its proof. We show that if f can be written as in (2) but $p \nmid m$ and $m_1 = m - 1$, then f can be written as in (1) for a different choice of g. We have $f = g^{m-1}(g + pw)$. Putting $g_2 = g + pu$ where u is any polynomial such that $\overline{u} = (\overline{m})^{-1}\overline{w}$ one can verify that $f = g_2^m$.

Assume now, for a contradiction, that f admits both a factorisation of type (i), say $f = g_1^m$ and a factorisation of type (ii), say $f = g^{m_1}(g^{m-m_1} + pw)$. Since $\overline{g} = \overline{g_1} = G$, there is a $u \in \mathrm{GR}(p^2, r)[x]$ so that $g_1 = g + pu$. Hence $g^m + pg^{m_1}w = (g + pu)^m = g^m + pmg^{m-1}u$, so $\overline{w} = \overline{m}\,\overline{g}^{m-m_1-1}\overline{u}$. We deduce that if $p|m$ then $\overline{w} = 0$ and if $p \nmid m$ then $m - m_1 - 1 \geqslant 1$ hence $G|\overline{w}$. But then, by Corollary 4.3, $g^{m-m_1} + pw$ would not be irreducible, so we obtain a contradiction.

Next we prove the assertions about the number of factors. For (i) it is obvious that the number of (non-distinct) factors is maximal, and that the number of distinct factors is one, therefore minimal. For (ii) consider an arbitrary factorisation of f into irreducible factors. It will have the form $f = \prod_{i=1}^{s}(g^{k_i} + pw_i)$ with $1 \leqslant k_1 \leqslant k_2 \leqslant \cdots \leqslant k_s$, $\sum_{i=1}^{s} k_i = m$, $w_i \in \mathrm{GR}(p^2, r)[x]$ and $g^{k_i} + pw_i$ irreducible. From $f = g^m + p\sum_{i=1}^{s} w_i g^{m-k_i} = g^m + pg^{m_1}w$ we deduce $\overline{g}^{m-k_s}\sum_{i=1}^{s}\overline{w_i}\,\overline{g}^{k_s-k_i} = \overline{g}^{m_1}w$. Hence $m - k_s \leqslant m_1$. Since $\sum_{i=1}^{s-1} k_i = m - k_s \leqslant m_1$, we deduce that $s \leqslant m_1 + 1$, so $m_1 + 1$ is the maximal number of factors in any factorisation of f. We also note that

the equality $s = m_1 + 1$ (i.e. factorisation into a maximal number of factors) can only be reached when $k_1 = k_2 = \cdots = k_{s-1} = 1$ and $k_s = m - m_1$. As factorisations of the form (ii) cannot be written in the form (i), the number of distinct irreducible factors has to be at least two.

Given a factorisation of f of type (i) or (ii) we will examine now what happens for a different choice of g with $\overline{g} = G$. Let g_1 be another polynomial such that $\overline{g}_1 = G$. There is a $u \in \mathrm{GR}(p^2, r)[x]$ so that $g = g_1 + pu$ and $pu \neq 0$. If f is in case (i) we have $f = (g_1 + pu)^m = g_1^m + pmg_1^{m-1}u$. This means that if $p|m$ then g_1 satisfies (1), otherwise it does not. If f is in case (ii) we have $f = (g_1 + pu)^m + p(g_1 + pu)^{m_1}w = g_1^m + p(mg_1^{m-1}u + g_1^{m_1}w) = g_1^{m_1}(g_1^{m-m_1} + pw_1)$, where we denoted $w_1 = mg_1^{m-1-m_1}u + w$. One can prove that $g_1^{m-m_1} + pw_1$ is irreducible either using Corollary 4.3 or using the fact that $m_1 + 1$ is the maximum number of factors of f, so any factorisation into $m_1 + 1$ factors can only contain irreducible factors.

It is easy to verify that these constructions give all the possible factorisations satisfying the stated requirements regarding the number of factors. □

We note that in the above theorem, if f is in case (ii) or if f is in case (i) and $p|m$, there are $|\mathrm{GF}(p^r)|^{\deg(g)}$ ways of choosing a monic g with $\overline{g} = G$. Hence, up to multiplication by units, there are $|\mathrm{GF}(p^r)|^{\deg(g)}$ factorisations satisfying the property in the theorem regarding the number of factors.

Based on Theorems 4.1 and 4.4 we can now develop an algorithm for deciding if a primary polynomial factors, and, in the affirmative case, obtaining a factorisation into the maximum number of irreducible factors.

Algorithm 4.5 (*Factorisation of a primary polynomial*).

Input: $f \in \mathrm{GR}(p^2, r)[x]$, a primary polynomial.
Output: A list of pairs $((f_1, m_1), \ldots, (f_s, m_s))$ so that $f = f_1^{m_1} \ldots f_s^{m_s}$ and f_i are irreducible or one of the messages "f is irreducible" or "f is basic irreducible".
Note: The factorisation has the maximum number of factors; among all factorisations into the maximum number of factors, this has the minimum number of distinct factors.

begin
Determine $G \in \mathrm{GF}(p^r)[x]$ and $m \geqslant 1$ so that $\overline{f} = G^m$ and G is irreducible.
if $m = 1$ **then return**("f is basic irreducible")
Choose $g \in \mathrm{GR}(p^2, r)[x]$ monic so that $\overline{g} = G$ and determine h so that $ph = f - g^m$.
if $\overline{h} = 0$ **then return**$(((g, m)))$
Determine the maximum m_1 so that $G^{m_1} | \overline{h}$ and determine w so that $\overline{h} = G^{m_1}\overline{w}$.
if $m_1 = 0$ **then return**("f is irreducible")
if $(p|m)$ or $(m_1 \leqslant m - 2)$ **then return**($((g, m_1), (g^{m-m_1} + pw, 1))$)
Choose u such that $\overline{u} = (\overline{m})^{-1}\overline{w}$.
return$(((g + pu, m)))$
end

It is easy to see that the worst-case complexity of the algorithm above is quadratic in the degree of f. Once a factorisation has been obtained, one can easily write down all possible factorisations having the properties in Theorem 4.4. Let us now apply the algorithm to an example:

Example 4.6. Let $f = x^3+6x^2+4 \in \mathbb{Z}_9[x]$. In $\mathbb{Z}_3[x]$ we have $\overline{f} = x^3+1 = (x+1)^3$. Hence f is primary but it is not basic irreducible. Put $g = x+1 \in \mathbb{Z}_9[x]$, $m = 3$ and $h = x^2+2x+1$. Since $\overline{h}$ is divisible by $\overline{g}^2$ and $p|m$, a factorisation of f into irreducible factors is $f = (x+1)^2(x+4)$. By taking all other possible values for g so that $\overline{g} = x+1$ we get all the other factorisations of f of this type, namely $f = (x+4)^2(x+7)$ and $f = (x+7)^2(x+1)$. Note that when viewed as a polynomial over the 3-adic numbers, f is irreducible (for example f has no roots in $\mathbb{Z}_{27}$ so it is irreducible in $\mathbb{Z}_{27}$ already). Hence none of these factorisations could be obtained by projecting to $\mathbb{Z}_9[x]$ the factorisation of f over the 3-adic numbers.

Using Theorem 4.4 and its proof, one can also obtain all the factorisations of a primary polynomial into the maximum number of irreducible factors (without the restriction on having a minimal number of distinct factors):

Corollary 4.7. *Let $f \in \mathrm{GR}(p^2, r)[x]$ be a monic primary polynomial which is not irreducible.*

(i) *Assume f admits a factorisation $f = g^m$ as in Theorem* 4.4(i). *Then $f = \prod_{i=1}^{m}(g + pw_i)$ with $w_i \in \mathrm{GR}(p^2, r)[x]$ arbitrary of degree less than* $\deg(g)$, *for $i = 1, \ldots, m-1$ and $w_m = -\sum_{i=1}^{m-1} w_i$, gives all the possible factorisations of f into a maximum number of monic irreducible factors.*

(ii) *If f admits a factorisation $f = g^{m_1}(g^{m-m_1} + pw)$ as in Theorem* 4.4(ii), *then $f = (\prod_{i=1}^{m_1}(g + pw_i))(g^{m-m_1} + pw_{m_1+1})$ with $w_i \in \mathrm{GR}(p^2, r)[x]$ arbitrary of degree less than* $\deg(g)$ *for $i = 1, \ldots, m_1$, and $w_{m_1+1} = w - g^{m-m_1-1}\sum_{i=1}^{m_1} w_i$, gives all the factorisations of f into a maximum number of monic irreducible factors.*

Proof. One can immediately verify that the formulae above are indeed factorisations of f into the maximum number of factors, hence all factors will be irreducible.

Next we have to show that we obtain indeed all the possible factorisations into a maximum number of factors. For (i), this is immediate. For (ii), we noted in the proof of Theorem 4.4 that (with the notations from that proof), any factorisation into a maximum number of factors has to satisfy $k_1 = k_2 = \cdots = k_{s-1} = 1$ and $k_s = m - m_1$. □

Remark 4.8. Polynomials in $\mathrm{GR}(p^2, r)[x]$ may also factor into fewer than the maximum number of irreducible factors given by Theorem 4.4. For example, if $f = g^m$ with $m \geqslant 4$, we can write $f = (g^k + pu)(g^k - pu)g^{m-2k}$ for any $2 \leqslant k \leqslant m/2$ and any $u \in \mathrm{GR}(p^2, r)[x]$ so that $\deg(u) < \deg(g^k)$, $\overline{u} \neq 0$ and $\overline{g} \nmid \overline{u}$. This is a factorisation into $m - 2k + 2 < m$ irreducible factors. For example we have the two factorisations

$x^4 = (x^2+2)^2$ in $\mathbb{Z}_4[x]$ and x^2+2 is irreducible. We will not examine this type of factorisations any further in this paper.

Using Corollary 4.3, one can easily show that the converse of Proposition 3.5 holds for Galois rings of characteristic p^2:

Corollary 4.9. *Let $f \in \mathrm{GR}(p^2, r)[x]$ be such that $\overline{f}$ is not square-free. Let f_1, f_2 be any polynomials in $\mathrm{GR}(p^2, r)[x]$ such that $\overline{f_1}$ is the square-free part of $\overline{f}$ and $\overline{f} = \overline{f_1 f_2}$. Let $h \in \mathrm{GR}(p^2, r)[x]$ be such that $ph = f - f_1 f_2$. The factorisation of f into primary pairwise coprime factors (given by Theorem 2.3) is a factorisation into irreducible factors if and only if $\overline{h} \neq 0$ and $\overline{h}$ and $\overline{f_2}$ are coprime.*

We note an interesting connection between the factorisation of a polynomial f and $\mathrm{GR}(p^a, r)[x]/\langle f\rangle$ being a principal ideal ring.

Theorem 4.10. *Let $f \in \mathrm{GR}(p^a, r)[x]$.*

(i) *If $\mathrm{GR}(p^a, r)[x]/\langle f\rangle$ is a principal ideal ring then the factorisation of f into primary pairwise coprime factors (given by Theorem 2.3) is a factorisation into irreducible factors.*
(ii) *When $a = 2$, $\mathrm{GR}(p^2, r)[x]/\langle f\rangle$ is a principal ideal ring if and only if the factorisation of f into primary pairwise coprime factors (given by Theorem 2.3) is a factorisation into irreducible factors.*

Proof. With the notations of Proposition 3.5, we have that $\mathrm{GR}(p^a, r)[x]/\langle f\rangle$ is a principal ideal ring if and only if $\overline{h} \neq 0$ and $\overline{h}$ and $\overline{f_2}$ are coprime (see [3, Theorem 4]; also [11, Theorem 3.2, 12]). The result now follows from Proposition 3.5 for (i) and from Corollary 4.9 for (ii). □

Remark 4.11. Note that the converse of point (i) in the theorem above does not hold for $a > 2$. For example, one can check that although $f = (x+1)^4 + 4x \in \mathbb{Z}_8[x]$ is primary and irreducible (see Example 3.2), $\mathbb{Z}_8[x]/\langle f\rangle$ is not a principal ideal ring (for example the ideal $\langle x+1, 2\rangle$ is not principal).

5. Application: factoring $x^n - 1$ and $x^n + 1$

In this section we determine factorisations of $x^n - 1$ and of $x^n + 1$ into a maximal number of irreducible factors over $\mathrm{GR}(p^2, r)[x]$.

The polynomial $x^n - 1$ is important for numerous applications. Our motivation comes from coding theory, where cyclic codes over a Galois ring are ideals in $\mathrm{GR}(p^a, r)[x]/\langle x^n - 1\rangle$. Negacyclic codes are ideals in $\mathrm{GR}(p^a, r)[x]/\langle x^n + 1\rangle$. One usually assumes that n is not divisible by p, but the case when $p|n$, yielding the so-called repeated-roots codes, is also of interest.

When n is not divisible by p, the polynomial $x^n - 1$ has no multiple factors over $\mathrm{GF}(p^r)$. Hensel lifting will produce then a unique factorisation of $x^n - 1$ over $\mathrm{GR}(p^a, r)[x]$ with all factors basic irreducible. The same happens for $x^n + 1$.

Factoring $x^n - 1$ (or $x^n + 1$) is more complicated when $p|n$. Here we deal with this case in rings of the form $\mathrm{GR}(p^2, r)$ (these rings include in particular $\mathbb{Z}_4$, which is an important ring for coding theory applications).

Theorem 5.1. *Let $x^n - 1 \in \mathrm{GR}(p^2, r)[x]$ and assume $p|n$. Write n as $n = kp^b$ with $b \geqslant 1$ and $p \nmid k$. Let $h \in \mathrm{GR}(p^2, r)[x]$ be any polynomial such that*

$$\overline{h} = \begin{cases} 1 & \text{if } p = 2, \\ \sum_{i=1}^{p-2} \left(\sum_{j=1}^{i} j^{-1} \right) x^{ikp^{b-1}} & \text{if } p > 2. \end{cases}$$

Then

(i)
$$x^n - 1 = (x^k - 1)^{p^{b-1}} ((x^k - 1)^{(p-1)p^{b-1}} + ph)$$

and $\overline{h}$ is relatively prime to $x^k - 1$ in $\mathrm{GF}(p^r)[x]$.

(ii) *Let $x^k - 1 = \prod_{i=1}^{s} f_i$ be the factorisation of $x^k - 1$ into basic irreducible factors over $\mathrm{GR}(p^2, r)[x]$ and let $w_i \in \mathrm{GR}(p^2, r)[x]$ be such that $(x^k-1)^{(p-1)p^{b-1}} + ph = \prod_{i=1}^{s} (f_i^{(p-1)p^{b-1}} + pw_i)$ is the factorisation of $(x^k-1)^{(p-1)p^{b-1}} + ph$ into primary pairwise coprime factors. Then*

$$x^n - 1 = \prod_{i=1}^{s} f_i^{p^{b-1}} \left(f_i^{(p-1)p^{b-1}} + pw_i \right) \tag{3}$$

is a factorisation of $x^n - 1$ into the maximum number of (not necessarily distinct) irreducible factors; among all possible factorisations into the maximum number of irreducible factors, the factorisation above consists of the minimum number of distinct factors.

Proof. (i) In $\mathrm{GF}(p^r)[x]$ we have $x^n - 1 = (x^k - 1)^{p^b}$. Hence in $\mathrm{GR}(p^2, r)[x]$ we have $x^n - 1 = (x^k - 1)^{p^b} + pt$ for some polynomial t which we will now determine.

For any $0 < j < p^b$, we know by Kummer's theorem that $\binom{p^b}{j}$ is divisible by p^{b-c} (and by no higher power of p) where c is the highest exponent so that $p^c | j$. So in particular $\binom{p^b}{j} \equiv 0 \bmod p^2$ for all values $0 < j < p^b$ for which j is not divisible by p^{b-1}. When j is of the form $j = ip^{b-1}$ with $0 < i < p$, $\binom{p^b}{ip^{b-1}}$ is divisible by p but not by p^2.

We will treat the case $p = 2$ first:

$$\begin{aligned} 2t &= x^n - 1 - (x^k - 1)^{2^b} = x^n - 1 - (x^n + 2x^{k2^{b-1}} + 1) = -2(x^{k2^{b-1}} + 1) \\ &= 2(x^k - 1)^{2^{b-1}}. \end{aligned}$$

Therefore $x^n - 1$ can be written as in the theorem, with $\overline{h} = 1$ in this case.

Now we assume $p > 2$. We have

$$pt = x^n - 1 - (x^k - 1)^{p^b} = x^n - 1 - \sum_{i=0}^{p} \binom{p^b}{ip^{b-1}} x^{ikp^{b-1}} (-1)^{(p-i)p^{b-1}}$$

$$= -\sum_{i=1}^{p-1} \binom{p^b}{ip^{b-1}} x^{ikp^{b-1}} (-1)^{p-i}.$$

By Lemma A.1 in the Appendix, $\binom{p^b}{ip^{b-1}} \equiv pc_i \bmod p^2$ where $\overline{c_i} = (-1)^{i-1} i^{-1}$. Hence

$$\overline{t} = -\sum_{i=1}^{p-1} (-1)^{i-1} i^{-1} x^{ikp^{b-1}} (-1)^{p-i} = -\sum_{i=1}^{p-1} i^{-1} x^{ikp^{b-1}}.$$

In $\mathrm{GF}(p^r)[x]$ we divide $\overline{t}$ by $(x^k - 1)^{p^{b-1}} = x^{kp^{b-1}} - 1$. We obtain the remainder $-\sum_{i=1}^{p-1} i^{-1} = -\sum_{i=1}^{p-1} i = -p(p-1)/2 \equiv 0 \bmod p$ (as i^{-1} will take all values between 1 and $p-1$ when i varies from 1 to $p-1$) and the quotient

$$\overline{h} = -\sum_{i=0}^{p-2} \sum_{j=i+1}^{p-1} j^{-1} x^{ikp^{b-1}} = \sum_{i=1}^{p-2} \sum_{j=1}^{i} j^{-1} x^{ikp^{b-1}}$$

(here again we used the fact that $\sum_{i=1}^{p-1} i^{-1} \equiv 0 \bmod p$).

It remains to show that $\overline{h}$ is coprime to $x^k - 1$. Assume they had a common factor. Then they would have a common root ξ in a suitable extension field. As ξ is a root of $x^k - 1$, we have $\xi^k = 1$. Evaluating $\overline{h}$ at ξ we obtain

$$\overline{h}(\xi) = -\sum_{i=0}^{p-2} \sum_{j=i+1}^{p-1} j^{-1} = -\sum_{j=1}^{p-1} jj^{-1} = -\sum_{j=1}^{p-1} 1 = -(p-1) = 1.$$

Hence we obtain a contradiction, as ξ cannot be a root of $\overline{h}$.

(ii) By Corollary 4.9, $(x^k - 1)^{(p-1)p^{b-1}} + ph = \prod_{i=1}^{s} (f_i^{(p-1)p^{b-1}} + pw_i)$ is the factorisation of $(x^k - 1)^{(p-1)p^{b-1}} + ph$ into irreducible factors, as $\overline{h}$ is coprime to $x^k - 1$. Hence (3) is a factorisation into irreducible factors.

It remains to prove the assertions about the number of irreducible factors. The factorisation of $x^n - 1$ into monic primary pairwise coprime factors is unique (Theorem 2.3) and from (3) there are s primary pairwise coprime factors, namely $f_i^{p^{b-1}}$ $(f_i^{(p-1)p^{b-1}} + pw_i)$, for $i = 1, \ldots, s$. By Theorem 4.4, each of these factors is factored in (3) into a

maximal number of irreducible factors, and the number of distinct factors is minimal among all such factorisations. □

Using similar techniques one can determine a factorisation of x^n+1. Note that the cases $p=2$ and $p>2$ differ more substantially here.

Theorem 5.2. *Let $x^n+1 \in \mathrm{GR}(p^2,r)[x]$ and assume $p|n$.*

(i) *If $p=2$ then the factorisation of x^n+1 into primary pairwise coprime factors in $\mathrm{GR}(2^2,r)[x]$ (given by Theorem 2.3) is also a factorisation into irreducible factors.*

(ii) *Let $p>2$. Write n as $n=kp^b$ with $b \geqslant 1$ and $p \nmid k$. Let h be any polynomial such that $\overline{h}=\sum_{i=1}^{p-2}(-1)^i(\sum_{j=1}^{i} j^{-1})x^{ikp^{b-1}}$. Then $x^n+1=(x^k+1)^{p^{b-1}}((x^k+1)^{(p-1)p^{b-1}}+ph)$ and $\overline{h}$ is relatively prime to x^k+1 in $\mathrm{GF}(p^r)[x]$. Let $x^k+1=\prod_{i=1}^{s} f_i$ be the factorisation of x^k+1 into basic irreducible factors over $\mathrm{GR}(p^2,r)[x]$ and let $w_i \in \mathrm{GR}(p^2,r)[x]$ be such that $(x^k+1)^{(p-1)p^{b-1}}+ph=\prod_{i=1}^{s}(f_i^{(p-1)p^{b-1}}+pw_i)$ is the factorisation of $(x^k+1)^{(p-1)p^{b-1}}+ph$ into primary pairwise coprime factors. Then*

$$x^n+1=\prod_{i=1}^{s} f_i^{p^{b-1}}(f_i^{(p-1)p^{b-1}}+pw_i) \tag{4}$$

is a factorisation of x^n+1 into the maximum number of (not necessarily distinct) irreducible factors; among all possible factorisations into the maximum number of irreducible factors, the factorisation above consists of the minimum number of distinct factors.

Proof. We will use the same notations as in the proof of Theorem 5.1. (i) Assume $p=2$. Then $x^n+1=(x^k+1)^{2^b}+2t$ and $2t=2x^{k2^{b-1}}$. Obviously $\bar{t}=x^{k2^{b-1}}$ is non-zero and coprime to x^k+1. Hence by Corollary 4.9, the factorisation of x^n+1 into primary coprime factors is also a factorisation into irreducible factors.

(ii) Assume $p>2$. We have $x^n+1=(x^k+1)^{p^b}+pt$ with

$$\bar{t}=-\sum_{i=1}^{p-1}(-1)^{i-1}i^{-1}x^{ikp^{b-1}}=\sum_{i=1}^{p-1}(-1)^i i^{-1}x^{ikp^{b-1}}.$$

When dividing $\bar{t}$ by $(x^k+1)^{p^{b-1}}=x^{kp^{b-1}}+1$ in $\mathrm{GF}(p^r)$ we obtain the remainder zero and the quotient $\overline{h}$, which one can check that is relatively prime to x^k+1. The rest of the proof is similar to the proof of Theorem 5.1. □

Remark 5.3. We note that the results of Theorems 5.1 and 5.2 together with Corollary 4.9 imply in particular that $\mathrm{GR}(p^2,r)[x]/\langle x^n-1\rangle$ is not a principal ideal ring whereas

$\mathrm{GR}(p^2, r)[x]/\langle x^n + 1\rangle$ is a principal ideal ring if $p = 2$ but it is not a principal ideal ring when $p > 2$. We retrieve thus particular cases of [11, Theorem 3.4, 12].

Acknowledgments

I would like to thank Serpil Acar for her encouragement while writing this paper.

Appendix A

Lemma A.1. *Let p be a prime number, $b \geqslant 1$ and $0 < i < p$. We have*:

(i) $\binom{p^b}{ip^{b-1}} \equiv \binom{p}{i} \pmod{p^b}$,

(ii) *Let* $c = \binom{p}{i}/p \in \mathbb{Z}$ (*the division is exact*). *Then* $c \bmod p = (-1)^{i-1} i^{-1}$ *in* $\mathbb{Z}_p$.

Proof. (i) We will use the usual formula $\binom{n}{k} = \frac{n\cdot(n-1)\cdot\ldots\cdot(n-k+1)}{k!}$, separating the factors that are divisible by p^{b-1}:

$$\binom{p^b}{ip^{b-1}} = \frac{p^b \cdot (p-1)p^{b-1} \cdot \ldots \cdot (p-i+1)p^{b-1}}{p^{b-1} \cdot 2p^{b-1} \cdot \ldots \cdot ip^{b-1}}$$
$$\cdot \frac{(p^b-1)(p^b-2)\ldots(p^b-p^{b-1}+1)(p^b-p^{b-1}-1)\cdot\ldots\cdot(p^b-ip^{b-1}+1)}{1\cdot 2\cdot\ldots\cdot(p^{b-1}-1)(p^{b-1}+1)\cdot\ldots\cdot(ip^{b-1}-1)}.$$

We denote by A and B the first and the second fraction above, respectively. For A we have in $\mathbb{Z}$

$$A = \frac{p(p-1)\cdot\ldots\cdot(p-i+1)}{i!} = \binom{p}{i}.$$

Obviously A is divisible by p. So for evaluating $AB \bmod p^b$ it suffices to evaluate $B \bmod p^{b-1}$. One can check that, modulo p^{b-1}, both the numerator and the denominator of B equal $(p^{b-1}-1)!\cdot i$, so $B \bmod p^{b-1} = 1$.

(ii) We have $c = \frac{(p-1)(p-2)\cdot\ldots\cdot(p-i+1)}{i!}$, so $c \bmod p = \frac{(-1)(-2)\cdot\ldots\cdot(-(i-1))}{i!} = (-1)^{i-1} i^{-1}$ in $\mathbb{Z}_p$. □

References

[1] E.R. Berlekamp, Factoring polynomials over large finite fields. Math. Comp. 24 (1970) 713–735.
[2] D.G. Cantor, D.M. Gordon, Factoring polynomials over *p*-adic fields, in: W. Bosma (Ed.), Algorithmic Number Theory, Fourth International Symposium, ANTS-IV, Leiden, The Netherlands, July 2–7, 2000, Proceedings, Lecture Notes in Computer Science, Vol. 1838, Springer, Berlin, 2000, pp. 5–7.

[3] J. Cazaran, A.V. Kelarev, Generators and weights of polynomial codes, Arch. Math. 69 (1997) 479–486.
[4] A.L. Chistov, Efficient factorisation of polynomials over local fields, Sov. Math. Dokl. 35 (1987) 430–433.
[5] A.L. Chistov, Algorithm of polynomial complexity for factoring polynomials over local fields, J. Math. Sci. 70 (1994) 1912–1933.
[6] D. Ford, S. Pauli, X.-F. Roblot, A fast algorithm for polynomial factorization over $\mathbb{Q}_p$, J. Th. Nombres Bordeaux 14 (2002) 151–169.
[7] D.J. Ford, The construction of maximal orders over a Dedekind domain, J. Symbolic Comput. 4 (1987) 69–75.
[8] A.R. Hammons Jr., P.V. Kumar, A.R. Calderbank, N.J.A. Sloane, P. Solé, The $\mathbb{Z}_4$ linearity of Kerdock, Preparata, Goethals and related codes, IEEE Trans. Inform. Theory 40 (1994) 301–319.
[9] B.R. McDonald, Finite Rings with Identity, Marcel Dekker, New York, 1974.
[10] S. Pauli, Factoring polynomials over local fields, J. Symbolic Comput. 32 (2001) 523–547.
[11] A. Sălăgean, Repeated-root cyclic and negacyclic codes over a finite chain ring, in: Proceedings of the Workshop on Coding and Cryptography, Paris, 24–28 March 2003, pp. 417–424.
[12] A. Sălăgean, Repeated-root cyclic and negacyclic codes over a finite chain ring, Discrete Appl. Math., in press.
[13] J. von zur Gathen, S. Hartlieb, Factoring modular polynomials, J. Symbolic Comput. 26 (1998) 583–606.