J. Korean Math. Soc. **44** (2007), No. 3, pp. 697–706

CYCLIC CODES OF EVEN LENGTH OVER $\mathbb{Z}_4$

SUNG SIK WOO

ABSTRACT. In [8], we showed that any ideal of $\mathbb{Z}_4[X]/(X^{2^n}-1)$ is generated by at most two polynomials of the standard forms. The purpose of this paper is to find a description of the cyclic codes of even length over $\mathbb{Z}_4$ namely the ideals of $\mathbb{Z}_4[X]/(X^l-1)$, where l is an even integer.

§ 1. Introduction

The ideals of $\mathbb{Z}_{p^n}[X]/(X^m-1)$ are called the *cyclic codes* of length m over $\mathbb{Z}_{p^n}$. When m is prime to p, a complete description of the cyclic codes of length m over $\mathbb{Z}_{p^n}$ is given in [5].

When $p^n = 4$ and m is of the form $m = 2^k$, it was shown that $S' = \mathbb{Z}_4[X]/(X^{2^k}-1)$ is isomorphic to $S = \mathbb{Z}_4[X]/(X^{2^k}-2X^{2^{k-1}})$ and the ideals of the later ring can be generated by at most two elements of some special type [8]. More generally, the ideals of a ring S which is generated by a nilpotent element x over $\mathbb{Z}_{p^2}$ can be generated by at most two elements of the similar type [9].

The purpose of this paper is to find the cyclic codes of even length over $\mathbb{Z}_4$, that is the ideals of $\mathbb{Z}_4[X]/(X^l-1)$ with $l = 2^n m, n \geq 1, m$ odd. We start with more general setting (§2), namely we consider a finite ring S with characteristic p which is a prime and we consider polynomials $S[T]$ over S. And in §3, we consider the ideals of a ring of type $S[T]/(f)$. In §4, we specialize to the rings S which is generated by a nilpotent element over $\mathbb{Z}_{p^2}$ and find the ideals of the ring of the form $S[T]/(f)$.

And then we further specialize to $p^2 = 4$ (§5) in which case $\mathbb{Z}_4[X]/(X^l-1)$ is isomorphic to the type $S[Y]/(Y^m-\bar{t}-1)$, where $l = 2^n m, n \geq 1, m$ is odd and S is a ring considered before. Since it is, in general, difficult to find a factorization of a polynomial over a commutative ring, we reduce the polynomials modulo the maximal ideal and find factorization over a field and then lift the factorization into polynomials over a commutative ring. In the final section (§6) we give some examples.

Received January 16, 2006.
2000 *Mathematics Subject Classification.* 13M05, 13M10.
Key words and phrases. cyclic code of even length over $\mathbb{Z}_4$.

A ring means a commutative ring with the identity 1 throughout this paper. The *characteristic* of a ring R is the smallest nonnegative integer n such that $nx = 0$ for all $x \in R$. The characteristic of a ring is assumed to be a prime p.

Acknowledgment. While this paper was prepared the author was unaware of the results of [1, 3]. On submission of this paper the referee pointed out these papers as well as [4]. This is the revised version of the original paper after the author was able to access to those papers. The results of this paper are not new anymore. The publication of the paper could be justified by the fact that the current paper used different methods from what they used in [1, 3].

In [4], they studied cyclic codes of length pm over Z_{p^n} whereas the author also worked out on the same problem in [10].

§ 2. Polynomial over a finite local ring

We collect the basic results on polynomials over a finite local rings for later use. Most of the result of this section should be well known and could be found somewhere else. We sometimes include their proofs just for completeness.

Recall some of the basic definitions on finite local rings in [7]. Let S be a finite local ring with the maximal ideal $\mathfrak{m}$. Since S is an Artin ring, $\mathfrak{m}$ is nilpotent ([2, Ch.8]). Also $\mathfrak{m}$ is finitely generated whose generators are also nilpotent. Hence every element of $\mathfrak{m}$ is nilpotent as well. Let $\mu : S \to S/\mathfrak{m}$ be the natural map and let $k = S/\mathfrak{m}$ be the residue field. A polynomial $f(T) \in S[T]$ is called *regular* if the coefficients of f generates the unit ideal of S. And f is called *basic irreducible* if $\mu(f) \in k[T]$ is irreducible. Obviously a basic irreducible polynomial is irreducible. As in [7], we denote J the set of polynomials f in $S[T]$ such that $\mu(f)$ has no multiple root in the algebraic closure of k.

Typical examples are $S = \mathbb{Z}_{p^2}[X]/(f(X))$, where $f(X)$ is a monic polynomial of degree m such that $X^n \in (p(X))$ for some n, i.e., $S = \mathbb{Z}_{p^2}[x]$ with $x^n = 0$ for some n. Note that S is a finite local ring with the maximal ideal (p, x). Later we specialize to the rings of the form $S = \mathbb{Z}_4[X]/(X^{2^n} - 2X^{2^{n-1}})$ which will turn out to be isomorphic to $S = \mathbb{Z}_4[X]/(X^{2^n} - 1)$.

Lemma 1 ([5], Corollary 2.5). *Let $f \in S[T]$ be regular and $f \in J$. Then*

(a) *$f = \delta g_1 \cdots g_n$, where δ is a unit in R and $g_1, \ldots, g_n$ are regular basic irreducible coprime polynomials.*

(b) *If $f = \delta g_1 \cdots g_n = \beta h_1 \cdots h_m$, where β and δ are units and $\{g_i\}$ and $\{h_j\}$ are regular basic irreducible coprime ideals then $n = m$ and, after renumbering $(h_i) = (g_j)$ $(1 \le i \le n)$.*

Proof. In [5], g_i's were primary instead of basic irreducible which should be what they intended. An easy complement goes as follows: By [7, Proposition XIII.12], a primary polynomial g_i is of the form $\delta \Pi^h + \beta$, where δ is a unit, Π a basic irreducible. If $h > 1$ then $\mu(f)$ must have a multiple root which contradicts to the fact that $f \in J$. □

We have an easy generalization of [5, Lemma 2.1]. Two polynomials f, g in $S[X]$ will be called *coprime* if f and g generate the unit ideal.

Lemma 2. *If f, g are regular then they are coprime if and only if $\mu(f)$ and $\mu(g)$ are coprime.*

Proof. If f, g are coprime then there are f_1, g_1 such that $ff_1 + gg_1 = 1$. Hence by reading the coefficients of the polynomials in the equality modulo $\mathfrak{m}$ we see that $\mu(f), \mu(g)$ are coprime.

Conversely let $\mu(f), \mu(g)$ are coprime. Then there are $\bar{f}_1, \bar{g}_1 \in k[X]$ such that $\mu(f)\bar{f}_1 + \mu(g)\bar{g}_1 = 1$. Hence there are $f_1, g_1 \in S[X]$ such that $ff_1 + gg_1 - 1 \in \mathfrak{m}$. Since every element of $\mathfrak{m}$ is nilpotent, there is a nilpotent element $n \in \mathfrak{m}$ such that $ff_1 + gg_1 = 1 + n$. Since $1 + n$ is a unit we see that f, g are coprime. □

Recall some basic facts about roots of polynomials over a commutative ring R. Let $f(X) \in R[X]$. An element c in a ring containing R is a *root* of $f(X)$ if $f(c) = 0$, i.e., $f(X) = (X - c)^m g(X)$ with $m \geq 1$. If $m > 1$ (resp. $m = 1$) then we say that c is a *multiple root* (resp. *simple root*) of $f(X)$. Formal derivative of a polynomial $f(X) = \sum_{i=0}^{n} c_i X^i$ is given by $f'(X) = \sum_{i=1}^{n} i c_i X^{i-1}$ as usual. We need the following well known fact.

Lemma 3. *Let be a commutative ring R and $f(X) \in R[X]$. Then a root c of $f(X)$ is a multiple root if and only if $f(c) = f'(c) = 0$.*

For our purpose the following proposition will suffice.

Proposition 1. *Let S be a finite ring of characteristic p. Let $f(X) = X^m - u \in S[X]$, where u is a unit in S and m is not divisible by p. Then $f(X)$ is a product of regular basic irreducible coprime polynomials.*

Proof. Obviously $f(X)$ is regular. We need to show that $\mu(f)$ has no multiple root. Now $\mu(f) = T^m - \bar{u}$ and $\mu(f)' = mT^{m-1}$. Hence $m\mu(f) - t(\mu(f))' = m\bar{u}$ is nonzero in $k = \mathbb{F}_p$ since m is prime to p. Therefore $\mu(f)$ and $\mu(f)'$ has no common root. By Lemma 3, $f(X) \in J$. Now by Lemma 1, $f(X)$ is a product of regular basic irreducible coprime polynomials. □

For later use, we record an application of the proposition to some special polynomial.

Corollary. *Let S be of characteristic p. Let $f(X) = X^m - x - 1 \in S[X]$, where m is prime to p and $x \in S$ is nilpotent. Then $f(X)$ is a product of regular basic irreducible coprime polynomials.*

Proof. Since x is nilpotent $1 + x$ is a unit. Hence Proposition 1 applies to the polynomial $f(X) = X^m - x - 1$. □

§ 3. Ideals of $S[T]/(f)$

We generalize [5, Lemma 3.1] in the following form.

Lemma 4. *Let S be a finite local ring with the maximal ideal $\mathfrak{m}$. Let f be a basic irreducible in $S[T]$ and let $\pi : S \to S[T]/(f)$ be the natural map. If I is an ideal of $S[T]/(f)$ then there is an ideal J of S such that $I = \pi(J)$.*

Proof. We may assume I is a nonzero ideal. If I contains h such that $\mu(f)$ and $\mu(h)$ are coprime then by Lemma 2, f and h are coprime. Hence I is the unit ideal.

Now suppose for every $h \in I$ we have $\mu(h)$ is a multiple of $\mu(f)$. Then $h(T) - f(T)u(T) = s_h$ for some $s_h \in \mathfrak{m}, u(T) \in S[X]$. Hence reading modulo f we see that there is $s_h \in \mathfrak{m}$ such that $\pi(s_h) = h$. Let $\pi^{-1}(I) = J$. Now it is obvious that $\pi(J) = I$. □

We use the usual notation: If $f = f_1 f_2 \cdots f_r$ then we will write $\hat{f}_i = f/f_i$. We can easily generalize [5, Theorem 3.2] by using the Chinese Remainder Theorem.

Theorem 1. *Let $f = f_1 f_2 \cdots f_r$ be a product of basic irreducible pairwise coprime polynomials of $S[T]$. Let I be an ideal of $S[T]/(f)$ then there are ideals J_i of S such that $I = \sum_{i=1}^{r} J_i(\hat{f}_i)$.*

Proof. Since f_i's are pairwise coprime in $S[T]$, we see

$$(f) = (f_1) \cap (f_2) \cap \cdots \cap (f_r)$$

and $(f_i, f_j) = (1)$ for $i \neq j$. By the Chinese Remainder Theorem, we have an isomorphism

$$\phi : S[T]/(f) \xrightarrow{\cong} \bigoplus_{i=1}^{r} S[T]/(f_i).$$

Let $\phi_i(I)$ be the i-th factor of $\phi(I)$. Then since f_i's are basic irreducible, we see $\phi_i(I) \subseteq S[T]/(f_i)$ is of the form J_i for some ideal J_i of S. Now the corresponding ideal in $S[T]/(f)$ is $J_i(\hat{f}_i)$. Hence $I = \sum_{i=1}^{r} J_i(\hat{f}_i)$. □

Theorem 2. *If I is an ideal of $S[X]/(f)$, then there exist a collection pairwise coprime polynomials $F_1, F_2, \ldots, F_k$ such that $f = F_1 F_2 \cdots F_k$ and I is generated by $\{J_1(\hat{F}_1), J_2(\hat{F}_2), \ldots, J_k(\hat{F}_k)\}$ namely*

$$I = \sum_{i=1}^{k} J_i(\hat{F}_i).$$

Moreover the polynomials are unique in the sense that if $f = H_1 H_2 \cdots H_k$ and $\{J_1(\hat{H}_1), J_2(\hat{H}_2), \ldots, J_k(\hat{H}_k)\}$ then each F_i is an associate of H_i.

Proof. We can use the same method as the proof of [5, Theorem 3.4] replacing (p^i) by J_i. □

§ 4. Ideals of algebras generated by a nilpotent element over $\mathbb{Z}_{p^2}$

In this section, we consider a ring of the form $S = \mathbb{Z}_{p^2}[X]/(\alpha(X))$, where $\alpha(X)$ is a monic polynomial of degree m such that $X^n \in (\alpha(X))$ for some n, i.e., $S = \mathbb{Z}_{p^2}[x]$ with $x^n = 0$ for some n and $\alpha(x) = 0$ for some monic polynomial α. Typical examples we have in mind are $S = \mathbb{Z}_{p^2}[X]/(X^m - pX^n)$ with nonnegative integers $m \geq n$.

Whenever we talk about a polynomial $f(X)$ in $S = \mathbb{Z}_{p^2}[X]/(\alpha(X))$ we shall choose a representative with degree less than m. Throughout this section we fix the degree of $\alpha(X)$, say $\deg(\alpha(X)) = m$.

Definition. The polynomials of the form

$$g(X) = X^k + pa_hX^h + pa_{h-1}X^{h-1} + \cdots + pa_0$$

with $a_h, a_{h-1}, \ldots, a_0 \in \mathbb{Z}_{p^2}$ will be called an *xkp form*. And we will often denote the polynomial $pa_hX^h + pa_{h-1}X^{h-1} + \cdots + pa_0$ by $p \cdot h(X)$. Also let us call the element of the form pX^r a *pxr form*.

The next two results from [9] enables us to find the generators of ideals of the rings of the form $S = \mathbb{Z}_{p^2}[X]/(\alpha(X))$ considered in this section.

Proposition 2 ([9]). *Let J be an ideal of S contained in (p). Then J is of the form (pX^r) for some r.*

Let us agree that the degree of the zero polynomial is $-\infty$ and $X^k = 0$ if $k = -\infty$.

Theorem 3 ([9]). *Let J be an ideal of S which is not contained in (p). Let $g(X) = X^k + ph(X) \in J$ be the smallest xkp form in J and pX^r be the smallest pxr form in J. Then $J = (g(X), pX^r)$, where $-\infty \leq r < l$.*

Theorem 3 together with the method used in [5] we obtain the following result.

Theorem 4. *Let $f = f_1 f_2 \cdots f_r$ be a product of basic irreducible pairwise coprime polynomials of $S[T]$. Let I be an ideal of $S[T]/(f)$. Suppose $J_i = (g_i(x), px^{r_i})$ then the ideal I is generated by*

$$\sum_{i=1}^{k} g_i\hat{f}_i, \ \sum_{i=1}^{k} px^{r_i}\hat{f}_i.$$

In particular, the ideal I can be generated by two elements.

Proof. The ideal I is generated by $\{g_i\hat{f}_i, px^{r_i}\hat{f}_i\}$ $(i = 1, 2, \ldots, k)$. Write $g = \sum_{i=1}^{k} g_i\hat{f}_i$. First we show that each $g_i\hat{f}_i$ is a multiple of g. We can show this by using the same method in [5, Corollary 3.6]. In fact, since f_i and $\hat{f}_i$ are coprime we can find polynomials a_i, b_i such that $a_if_i + b_i\hat{f}_i = 1$ for all i.

Therefore $\prod_{i=1}^{l}(a_i f_i + b_i \hat{f}_i) = 1$ for $(1 \leq l \leq k)$. Multiplying this out we can write it in the form

$$a_{l0} f_1 f_2 \cdots f_l + a_{l1} \hat{f}_1 f_2 \cdots f_l + a_{l2} f_1 \hat{f}_2 \cdots f_l + \cdots + a_{ll} f_1 f_2 \cdots \hat{f}_l = 1$$

for some polynomials a_{ij}. Multiply both sides of the above equation by $g_k \hat{f}_k$ with $l = k-1$. Then we obtain

$$g_k \hat{f}_k = g_k a_{k-1,l} f_1 f_2 \cdots f_{k-1} \hat{f}_k.$$

On the other hand,

$$f_1 f_2 \cdots f_{k-1} g = g_k f_1 f_2 \cdots f_{k-1} \hat{f}_k.$$

Therefore $g_k \hat{f}_k \in (g)$. Hence $\sum_{i=1}^{k-1} g_i \hat{f}_i \in (g)$. Similarly, we can show that $px^{r_{k-1}} \hat{f}_{k-1} \in (g)$ which entails $\sum_{i=1}^{k-2} g_i \hat{f}_i \in (g)$. By repeating this process we conclude that $g_i \hat{f}_i \in (g)$ for each i.

The same method applied to px^{r_i} instead of g_i yields that $px^{r_i} \hat{f}_i$ is a multiple of $\sum_{i=1}^{k} px^{r_i} \hat{f}_i$. □

§ 5. The cyclic codes of even length over $\mathbb{Z}_4$

The cyclic codes of even length over $\mathbb{Z}_4$ are precisely the ideals of the finite local ring $\mathbb{Z}_4[X]/(X^l - 1)$ with $l = 2^n m, n \geq 1$, where m is odd. We first look at the ring $S' = \mathbb{Z}_4[X]/(X^{2^n} - 1)$. In [8], we showed that the ring $\mathbb{Z}_4[X]/(X^{2^n} - 1)$ is isomorphic to the ring $S = \mathbb{Z}_4[X]/(X^{2^n} - 2X^{2^{n-1}})$ whose ideals are generated at most two elements by Theorem 3.

The following lemma can be found in [1].

Lemma 5 ([1])**.** *Let $n \geq 1$. Let $X^{2^n} - 1 \in \mathbb{Z}_4[X]$. Then we can write*

$$X^{2^n} - 1 = (X-1)^{2^n} - 2(X-1)^{2^{n-1}}.$$

Corollary ([8])**.** *There is an isomorphism*

$$\psi : \mathbb{Z}_4[\overline{T}]/(\overline{T}^{2^n} - 2\overline{T}^{2^{n-1}}) \longrightarrow \mathbb{Z}_4[T]/(T^{2^n} - 1)$$

of rings which maps $f(\overline{T})$ to $f(T-1)$. The inverse of ψ maps $f(T)$ to $f(\overline{T}+1)$.

Let l be an even integer and write $l = 2^n m$, where m is an odd. We will show that $\mathbb{Z}_4[X]/(X^l - 1)$ is isomorphic to $S[T]/(T^m - t - 1)$, where $S = \mathbb{Z}_4[\overline{T}]/(\overline{T}^{2^n} - 2\overline{T}^{2^{n-1}})$. By Proposition 2 and Theorem 3, we have a complete description of the ideals of S. By Corollary to Proposition 1, $T^m - t - 1 \in S[T]$ can be factored into regular basic irreducible pairwise coprime polynomials. We can then use Theorem 4 to get the ideals of $S[T]/(T^m - x - 1)$.

Theorem 5. *With the notations above we have an isomorphism*

$$\mathcal{U} : \mathbb{Z}_4[X]/(X^l - 1) \to S[Y]/(Y^m - \bar{t} - 1),$$

where $S = \mathbb{Z}_4[\overline{T}]/(\overline{T}^{2^n} - 2\overline{T}^{2^{n-1}})$ and $\bar{t}$ denotes the canonical image of $\overline{T}$ in S.

Proof. Let $S' = \mathbb{Z}_4[T]/(T^{2^n} - 1)$. By letting $T = X^m$, we can identify $\mathbb{Z}_4[X]/((X^m)^{2^n} - 1) = \mathbb{Z}_4[T]/(T^{2^n} - 1)[\sqrt[m]{T}\,] = S'[\sqrt[m]{T}\,]$. And we have an isomorphism

$$\alpha : S'[\sqrt[m]{T}\,] \stackrel{\cong}{\to} S'[Y]/(Y^m - t),$$

where t is the canonical image of T in S'. Composing α with the isomorphism ψ of Corollary to Lemma 5, we have the desired isomorphism. □

To describe the isomorphism explicitly we follow the maps: First let choose a representative $f(X) \in \mathbb{Z}_4[X]/(X^l - 1)$. Write $f(X)$ in the form

$$f(X) = \sum_{i=0}^{m-1} \left(\sum_{j=0}^{2^n-1} a_{ij} t^j \right) X^i$$

with $t = X^m$ and $a_{ij} \in \mathbb{Z}_4$. Then $f(Y)$ can be viewed as an element of $S'[Y]$ and read modulo $Y^m - t$, namely view it as an element of $S'[Y]/(Y^m - t)$. Now the corresponding element of $S[Y]/(Y^m - \bar{t} - 1)$ will be

$$\mathcal{U}(f) = \sum_{i=0}^{m-1} \left(\sum_{j=0}^{2^n-1} a_{ij} (\bar{t} + 1)^j \right) Y^i.$$

The inverse map will be given as follows: Let $\sum_{i=0}^{m-1} s_i(\bar{t}) Y^i$ be an element of $S[Y]/(Y^m - \bar{t} - 1)$ with $s_i(\bar{t}) = \sum_{j=0}^{2^n-1} b_{ij} \bar{t}^j$, $b_{ij} \in \mathbb{Z}_4$. Write $s_i(\bar{t})$ in the form $s_i(\bar{t}) = \sum_{j=0}^{2^n-1} c_{ij} (\bar{t} + 1)^j$ with $c_{ij} \in \mathbb{Z}_4$. (This can be achieved by dividing $s_i(\bar{t}) = \sum_{j=0}^{2^n-1} b_{ij} \bar{t}^j$ by the powers $(\bar{t}+1)^{2^n-1}, (\bar{t}+1)^{2^n-2}, \cdots$ of $(\bar{t}+1)$. Namely, $s_i(\bar{t}) = c_{i1}(\bar{t}+1)^{2^n-1} + R_1(\bar{t})$ and $R_1(\bar{t}) = c_{i2}(\bar{t}+1)^{2^n-2} + R_2(\bar{t})$ etc.) Now the corresponding element in $\mathbb{Z}_4[X]/(X^l - 1)$ will be

$$f(X) = \sum_{i=0}^{m-1} \left(\sum_{j=0}^{2^n-1} c_{ij} X^{mj} \right) X^i.$$

Summing up the discussion above, we state in the following proposition.

Proposition 3. *Under the isomorphism*

$$\mathcal{U} : \mathbb{Z}_4[X]/(X^l - 1) \to S[Y]/(Y^m - \bar{t} - 1).$$

For $f(X) \in \mathbb{Z}_4[X]/(X^l - 1)$, write it in the form $f(X) = \sum_{i=0}^{m-1} \left(\sum_{j=0}^{2^n-1} a_{ij} t^j \right) X^i$ with $t = X^m$. Then

$$\mathcal{U}(f) = \sum_{i=0}^{m-1} \left(\sum_{j=0}^{2^n-1} a_{ij} (\bar{t} + 1)^j \right) Y^i.$$

On the other hand, for $g(Y) = \sum_{i=0}^{m-1} s_i(\bar{t})Y^i \in S[Y]/(Y^m - \bar{t} - 1)$ *with* $s_i(\bar{t}) = \sum_{j=0}^{2^n-1} b_{ij}\bar{t}^j$, $b_{ij} \in \mathbb{Z}_4$. *If* $s_i(\bar{t}) = \sum_{j=0}^{2^n-1} c_{ij}(\bar{t}+1)^j$ *with* $c_{ij} \in \mathbb{Z}_4$ *then*

$$\mathcal{U}^{-1}(g(Y)) = \sum_{i=0}^{m-1} \left(\sum_{j=0}^{2^n-1} c_{ij} Y^{mj} \right) Y^i.$$

We want to look at the polynomial $Y^m - t \in S'[Y]$ more closely. By Proposition 1, we know that $Y^m - t$ is a product of basic irreducible polynomials. But it is, in general, very difficult to find such factorization in $S'[Y]$. But by reducing the polynomial $Y^m - \bar{t} - 1 \in S[Y]$ modulo $\mathfrak{m}$ we obtain a polynomial $Y^m - 1 \in \mathbb{F}_2[Y]$ which we can factor into irreducible polynomials rather easily. And then we can use Hensel's Lemma to lift such factorization to $S'[Y]$.

Now we recall some basic facts about roots of unity and cyclotomic polynomials from [6]. Let F be a field of characteristic $p > 0$ and m be a positive integer. Let $F^{(m)}$ be the splitting field of $X^m - 1$ over F and μ_m be the set of m-th roots of unity. If $(m, p) = 1$ then μ_m is a cyclic group of order m [6, p.59]. Let ζ be a primitive m-th root of unity i.e., a generator of μ_m. We define the *m-th cyclotomic polynomial* to be

$$Q_m(X) = \prod_{(s,m)=1} (X - \zeta^s).$$

Then it is well known that $Q_m(X) \in \mathbb{F}_p[X]$ is a polynomial of degree $\phi(m)$, where $\mathbb{F}_p$ is the field of p elements, i.e., the prime field of F.

Theorem 6 ([6], pp.60-61). *Let* $F = \mathbb{F}_p$ *be the field of* p *elements and* m *be a positive integer not divisible by* p. *Then*

(i) $X^m - 1 = \prod_{k|m} Q_k(X)$.

(ii) *Let* d *be the least positive integer such that* $p^d \equiv 1 \mod m$. *Then* $Q_m(X)$ *factors into* $\phi(m)/d$ *irreducible polynomials in* $F[X]$ *of degree* d *and* $[F^{(m)} : F] = d$, *where* ϕ *is the usual Euler* ϕ *function.*

Now we want to use the Hensel's Lemma to lift the factorization of the polynomial $Y^m - 1 \in \mathbb{F}_2[Y]$ to the factorization of $Y^m - t \in S'[Y]$.

Hensel's Lemma [7]. *Let* S *be an Artin local ring with the maximal ideal* $\mathfrak{m}$. *Let* $k = S/\mathfrak{m}$ *be the residue field and* $\mu : S \to k$ *be the natural map. Let* $P(X) \in S[X]$ *be a polynomial. Let* $g \in k[X]$ *be a monic polynomial and* $h(X) \in k[X]$ *be a polynomial such that* g, h *are coprime. Suppose that* $\mu(P) = g \cdot h$. *Then there exist unique coprime polynomials* $G, H \in S[X]$ *such that* $\mu(G) = g, \mu(H) = h$ *and* $P(X) = G(X)H(X)$ *in* $S[X]$.

Using the isomorphism of Theorem 5, we apply these results with the Artin local ring $S = \mathbb{Z}_4[\overline{T}]/(\overline{T}^{2^n} - 2\overline{T}^{2^{n-1}})$ and $p = 2$ to find the ideals of $\mathbb{Z}_4[X]/(X^l - 1)$.

Theorem 7. *Let $l = 2^n m$ with $n \geq 1$ and m odd. For each divisor k of m let d_k be the smallest positive integer such that $2^{d_k} \equiv 1 \pmod{k}$. Then $Y^m - \bar{t} - 1$ is a product of $\sum_{k|m} \frac{\phi(k)}{d_k}$ irreducible polynomials $\{f_1, f_2, \ldots, f_t\}$ in $S[Y]$, where $S = \mathbb{Z}_4[\overline{T}]/(\overline{T}^{2^n} - 2\overline{T}^{2^{n-1}})$. Further, we have an isomorphism*

$$\mathbb{Z}_4[X]/(X^l - 1) \xrightarrow{\cong} \bigoplus_{i=1}^{t} S[Y]/(f_i)$$

and the ideals of $S[Y]/(f_i)$ comes from the ideals of S which are generated by at most two elements.

Proof. By Theorem 6 and the Hensel's Lemma we have the required factorization of $Y^m - \bar{t} - 1$. By Theorem 2, the ideals of $S[Y]/(f_i)$ comes form the ideals of S and by Theorem 3, they are generated by at most two elements. □

§ 6. Examples

Example 1. Consider $X^{12} - 1 \in \mathbb{Z}_4[X]$. Let $S' = \mathbb{Z}_4[T]/(T^4 - 1)$. Then S' is a local ring with the maximal ideal $\mathfrak{m}' = (2, t - 1)$ and we can identify $\mathbb{Z}_4[X]/(X^{12} - 1)$ with $\mathbb{Z}_4[T]/(T^4 - 1)[\sqrt[3]{T}\,] = S'[\sqrt[3]{T}\,]$. Now this is isomorphic to $S'[Y]/(Y^3 - t)$, where t is the canonical image of T in S'. The polynomial $Y^3 - t \in S'[Y]$ has factorization

$$Y^3 - t = (Y - t^3)(Y^2 + t^3 Y + t^2).$$

Reading the polynomial $Y^2 + t^3 Y + t^2$ modulo $\mathfrak{m}'$ we see $\mu(Y^2 + t^3 Y + t^2) = Y^2 + Y + 1 \in \mathbb{F}_2[Y]$. Hence the polynomials in the factorization above are coprime basic irreducibles. Hence $Y^3 - (\bar{t} + 1) \in S[Y]$ has factorization into coprime basic irreducibles

$$Y^3 - (\bar{t} + 1) = (Y - (\bar{t} + 1)^3)(Y^2 + (\bar{t} + 1)^3 Y + (\bar{t} + 1)^2),$$

where $\mathbb{Z}_4[\overline{T}]/(\overline{T}^4 - 2\overline{T}^2)$.

Hence $\mathbb{Z}_4[X]/(X^{12} - 1)$ is isomorphic to

$$S[Y]/(Y - (\bar{t} + 1)^3) \oplus S[Y]/(Y^2 + (\bar{t} + 1)^3 Y + (\bar{t} + 1)^2)$$

and the ideals of each factor comes from the ideals of S.

Example 2. Consider $X^{36} - 1 \in \mathbb{Z}_4[X]$. Let $S' = \mathbb{Z}_4[T]/(T^4 - 1)$. Then $\mathbb{Z}_4[X]/(X^{36} - 1) \cong S'[Y]/(Y^9 - t)$. Reading the polynomial $Y^9 - t \in S'[Y]$ modulo $\mathfrak{m}$, we get $Y^9 - 1 \in \mathbb{F}_2[X]$. By Theorem 6, $Y^9 - 1 = Q_1 Q_3 Q_9$. By using [6, p.61],

$$Q_{p^k}(Y) = 1 + Y^{p^{k-1}} + Y^{2p^{k-1}} + \cdots + Y^{(p-1)p^{k-1}}$$

we obtain $Q_1(Y) = Y - 1$, $Q_3(Y) = 1 + Y + Y^2$, $Q_9(Y) = 1 + Y^3 + Y^6$. Clearly $Q_3(Y) \in \mathbb{F}_2[Y]$ is irreducible. By Theorem 6, $Q_9(Y)$ is a product of $\phi(9)/d$ irreducible polynomials, where d is the smallest positive integer such

that $2^d \equiv 1 (\mathrm{mod}\ 9)$. Since $d = 6$ and $\phi(9) = 6$ we see that $Q_9(Y)$ is irreducible. Therefore we have a factorization

$$Y^9 - 1 = (Y-1)(Y^2+Y+1)(Y^6+Y^3+1)$$

into irreducible factors in $\mathbb{F}_2[Y]$. By Hensel's Lemma we can lift this factorization on $S'[Y]$. In fact,

$$Y^9 - t = (Y-t)(Y^6+t^3Y^3+t^2)(Y^2+tY+t^2).$$

Therefore in $S[Y]$ we have

$$\begin{aligned} &Y^9 - (\bar{t}+1) \\ &= (Y-(\bar{t}+1))(Y^6+(\bar{t}+1)^3Y^3+(\bar{t}+1)^2)(Y^2+(\bar{t}+1)Y+(\bar{t}+1)^2). \end{aligned}$$

Therefore $\mathbb{Z}_4[X]/(X^{36}-1)$ is isomorphic to

$$S[Y]/(Y-s) \oplus S[Y]/(Y^6+s^3Y^3+s^2) \oplus S[Y]/(Y^2+sY+s^2),$$

where $s = \bar{t}+1$, $S = \mathbb{Z}_4[\overline{T}]/(\overline{T}^4 - 2\overline{T}^2)$ and $\bar{t}$ is the canonical image of $\overline{T}$ in S. The ideals of each factor are induced form the ideals of S which are of the form $J = (g(\bar{t}), 2\bar{t}^r)$, where $g(\bar{t}) = \bar{t}^k + 2h(\bar{t})$ is an $xk2$ form and $k, r \leq 4$.

References

[1] T. Abualrub and R. Oemke, *On the generators of $\mathbb{Z}_4$ cyclic codes of length 2^e*, IEEE Trans. Inform. Theory **49** (2003), no. 9, 2126–2133.

[2] M. F. Atiyah and I. G. Macdonald, *Introduction to Commutative Algebra*, Addison-Wesley, 1969.

[3] T. Blackford, *Cyclic codes over $\mathbb{Z}_4$ of oddly even length*, Discrete Appl. Math. **128** (2003), no. 1, 27–46.

[4] S. T. Dougherty and Y. H. Park, *On modular cyclic codes*, (Preprint), 2006.

[5] P. Kanwar and S. R. López-Permouth, *Cyclic codes over integer modulo p^n*, Finite Fields Appl. **3** (1997), no. 4, 334–352.

[6] R. Lidl and H. Niederreiter, *Introduction to finite fields and their applications*, Cambridge University Press, 1986.

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

[8] S. Woo, *Cyclic codes of length 2^n over $\mathbb{Z}_4$*, (Preprint), 2005.

[9] ———, *Algebras with a nilpotent generator over $\mathbb{Z}_{p^2}$*, Bull. Korean Maht. Soc. **43** (2006), no. 3, 487–497.

[10] ———, *Cyclic codes of length pm over $\mathbb{Z}_{p^n}$*, (Preprint), 2006.

Department of Mathematics
Ewha Women's University
Seoul 120-750, Korea
E-mail address: sswoo@ewha.ac.kr