Korean J. Math. **27** (2019), No. 3, pp. 767–777
https://doi.org/10.11568/kjm.2019.27.3.767

CYCLIC CODES OVER THE RING OF 4-ADIC INTEGERS OF LENGTHS 15, 17 AND 19

Young Ho Park

Abstract. We present a new way of obtaining the complete factorization of $X^n - 1$ for $n = 15, 17, 19$ over the 4-adic ring $\mathcal{O}_4[X]$ of integers and thus over the Galois rings $GR(2^e, 2)$. As a result, we determine all cyclic codes of lengths 15, 17 and 19 over those rings. This extends our previous work on such cyclic codes of odd lengths less than 15.

1. Introduction

Let $\mathbb{F}_q$ denote the finite field of $q = p^r$ elements with characteristic p. In our previous work [9], we presented a theoretical background for q-adic liftings of cyclic codes over $\mathbb{F}_q$ and determined all cyclic codes over $\mathbb{F}_4$ of length less than 15 and all liftings to the 4-adic ring of integers. In this article, we continue this work to determine liftings of cyclic codes of length $15, 17, 19$.

For generality on codes over fields, we refer to [5, 7]. See [2, 8] for codes over $\mathbb{Z}_m$, and [2, 3] for codes over p-adic rings.

We will use the same notations as in [9]. So $GR(p^e, r)$ denotes a Galois ring, $\mathbb{Q}_p$ denotes the p-adic field and $\mathcal{O}_p$ its ring of integers. $\mathbb{Q}_{p^r}$ denotes the unique unramified extension of degree r over $\mathbb{Q}_p$ and $\mathcal{O}_{p^r}$ denotes the ring of integers of $\mathbb{Q}_{p^r}$.

Received July 23, 2019. Revised September 5, 2019. Accepted September 8, 2019.
2010 Mathematics Subject Classification: 94B05, 11T71.
Key words and phrases: Cyclic codes, Galois rings, q-adic codes, Lifting.
This work was supported by 2017 Research Grant from Kangwon National University (No. 520170501).
© The Kangwon-Kyungki Mathematical Society, 2019.
This is an Open Access article distributed under the terms of the Creative commons Attribution Non-Commercial License (http://creativecommons.org/licenses/by-nc/3.0/) which permits unrestricted non-commercial use, distribution and reproduction in any medium, provided the original work is properly cited.

There exists a projective system

$$\mathbb{F}_{p^r} \longleftarrow GR(p^2, r) \longleftarrow GR(p^3, r) \longleftarrow \cdots \longleftarrow \mathcal{O}_{p^r}. \tag{1}$$

and an isomorphism between Galois groups

$$\mathrm{Gal}(GR(p^e, rs)/GR(p^e, r)) \simeq \mathrm{Gal}(\mathcal{O}_{p^{rs}}/\mathcal{O}_{p^r}) \tag{2}$$

generated by $\mathtt{Fr}^r$ given by

$$\mathtt{Fr}^r(a_0 + a_1 p + \cdots + a_t p^t + \cdots) = a_0^{p^r} + a_1^{p^r} p + \cdots + a_t^{p^r} p^t + \cdots$$

on the p-adic expansion. In particular, if α is any nth of unity in $\mathcal{O}_{p^{rs}}$, where $n \mid p^{rs} - 1$, then $\mathtt{Fr}^r(\alpha) = \alpha^{p^r}$. Recall that $\beta \in \mathcal{O}_{p^{rs}}$ lies in $\mathcal{O}_{p^r}$ if and only if $\mathtt{Fr}^r(\beta) = \beta$.

2. Factorization of $X^n - 1$

We always assume that n is an integer relatively prime to q. The order of q modulo n is the smallest positive integer t such that $q^t \equiv 1 \pmod{n}$. Then $\mathbb{F}_{q^t}$ contains a primitive nth root of unity α, but no smaller extension of $\mathbb{F}_q$ does.

Let $0 \le s \le n-1$. The q-cyclotomic coset of s modulo n is the set

$$C_s = \{s, sq, \cdots, sq^{m-1} \pmod{n}$$

where m is the smallest positive integer such that $sq^m \equiv s \pmod{n}$. Let

$$g_s(X) = \prod_{i \in C_s} (X - \alpha^i).$$

Then

$$X^n - 1 = \prod_s g_s(X)$$

is the factorization of $X^n - 1$ into irreducibles over $\mathbb{F}_q$, where s runs over a set of representatives of q-cyclotomic cosets. This factorization completely determines the cyclic codes of length n over $\mathbb{F}_q$. See [5, 7] for more detail.

Since any cyclic code of length n over $\mathbb{F}_q = \mathcal{O}_q/(p)$ is generated by a monic factor $g_1(X)$ of $X^n - 1$, where $X^n - 1 = g_1(X)g_2(X)$, Hensel's lemma [4, 9] provides a mechanism for generalizing any class of cyclic codes from $\mathbb{F}_q$ to $GR(p^e, r)$ by $X^n - 1 \equiv g_{1,e}(X)g_{2,e}(X) \pmod{p^e}$ and to $\mathcal{O}_q$ by $X^n - 1 = g_{1,\infty}(X)g_{2,\infty}h(X)$. See [1] for more detail.

3. Examples

We will consider the case $q = 2^2$ so that $p = 2$ and $r = 2$. As usual, $\mathbb{F}_4 = \{0, 1, \omega, 1+\omega\} = \{0, 1, \omega, \omega^2\}$, where ω is a root of the polynomial $\bar{h}(X) = X^2 + X + 1 \in \mathbb{F}_2[x]$ and $\mathbb{F}_4 = \mathbb{F}_2(\omega)$. Lift $\bar{h}(X)$ over $\mathcal{O}_2$ as $h(X) = X^2 + X + 1$. This is irreducible over $\mathcal{O}_2$ and over $\mathbb{Q}_2$ as well. Let ζ be a root of $h(X)$ in $\mathcal{O}_4$ so that $\mathcal{O}_4 = \mathcal{O}_2[\zeta]$. Since we may take ω as $\zeta \pmod 2$, we will replace ζ with ω. This way, the projections of $\zeta \in \mathcal{O}_4$ to $GR(2^2, 2)$ are all denoted by ω and we may write

$$\mathbb{F}_4 = \mathbb{F}_2[\omega], \quad GR(2^e, 2) = \mathbb{Z}_{p^e}[\omega], \quad \mathcal{O}_4 = \mathcal{O}_2[\omega], \quad \mathbb{Q}_4 = \mathbb{Q}_2[\omega].$$

3.1. Cyclic codes of length 15. First we will consider cyclic codes over $\mathbb{F}_4$ of length 15. The q-cyclotomic cosets mod $n = 15$ are given by

$$\begin{aligned} &C_0 = \{0\}, \quad C_1 = \{1,4\}, \quad C_2 = \{2,8\}, \quad C_3 = \{3,12\}, \quad C_5 = \{5\} \\ &C_6 = \{6,9\}, \quad C_7 = \{7,13\}, \quad C_{10} = \{10\}, \quad C_{11} = \{11,14\}. \end{aligned}$$

Thus $X^{15} - 1$ splits into linear factors over $\mathbb{F}_{4^2} = \mathbb{F}_2[\omega_2]$, where ω_2 is a root of $X^4 + X + 1$ over $\mathbb{F}_2$ of multiplicative order 15. Let $\alpha \in \mathbb{F}_{4^2}$ be any primitive 15th root of unity. We may take $\alpha = \omega_2$. Note also that $(\omega_2^5)^4 = \omega_2^5$, and hence $\mathbb{F}_4 = \{0, 1, \omega_2^5, \omega_2^{10}\}$. Thus we may take $\omega = \omega_2^5 = \omega_2^2 + \omega_2$. Let $g_s(X) = \prod_{i \in C_s}(X - \alpha^i)$ as before. Then $X^{15} - 1$ factors over $\mathbb{F}_4$ as follows:

$$X^{15} - 1 = (X-1)g_1(X)g_2(X)g_3(X)g_5(X)g_6(X)g_7(X)g_{10}(X)g_{11}(X).$$

It turns out that the factors $g_s(X)$ of $X^{15} - 1$ are

$$\begin{aligned} g_1(X) &= X^2 + X + \omega, & g_2(X) &= X^2 + X + (\omega+1) \\ g_3(X) &= X^2 + (\omega+1)X + 1, & g_5(X) &= X + \omega \\ g_6(X) &= X^2 + \omega X + 1, & g_7(X) &= X^2 + \omega X + \omega \\ g_{10}(X) &= X + (\omega+1), & g_{11}(X) &= X^2 + (\omega+1)X + (\omega+1) \end{aligned}$$

To see these, we consider $g_3(X) = X^2 - (\alpha^3 + \alpha^{12})X + 1$ for example. By the division algorithm we have that

$$X^3 + X^{12} \equiv X^2 + X + 1 \pmod{X^4 + X + 1}$$

so that $\alpha^3 + \alpha^{12} = \omega_2^2 + \omega_2 + 1 = \omega + 1$.

We would like to lift $g_s(X)$ to $g_{s,e}(X) \in GR(2^e, 2)[X]$ for all $e = 2, 3, \cdots$ such that

$$X^{15} - 1 = (X - 1)\prod_s g_{s,e}(X).$$

Using the software like MAGMA [6], we can obtain $g_{s,e}$ for small e's. For example, we list $g_{s,5}$ over $GR(32, 2)$:

$$\begin{aligned}
&g_{1,5}(X) = X^2 + (6\omega - 7)X + \omega, && g_{2,s}(X) = X^2 + (-6\omega - 13)X - (\omega + 1)\\
&g_{3,5}(X) = X^2 + (13\omega + 7)X + 1, && g_{5,5}(X) = X - \omega\\
&g_{6,5}(X) = X^2 + (-13\omega - 6)X + 1, && g_{7,5}(X) = X^2 + (-7\omega + 6)X + \omega\\
&g_{10.5}(X) = X + \omega + 1, && g_{11,5}(X) = X^2 + (7\omega + 13)X - (\omega + 1)
\end{aligned}$$

However, it is impossible to get their lifts in this way to the 4-adic ring. Instead, by a careful inspection of lifts of $g_s(X)$ for small e's we first conjecture that the q-adic lifts will have the form

$$\begin{aligned}
g_{1,\infty}(X) &= X^2 + (a\omega + b)X + \omega,\\
g_{2,\infty}(X) &= X^2 + (-a\omega + (b - a))X - (\omega + 1)\\
g_{3,\infty}(X) &= X^2 + ((a - b)\omega - b)X + 1,\\
g_{5,\infty}(X) &= X - \omega\\
g_{6,\infty}(X) &= X^2 + ((b - a)\omega - a)X + 1,\\
g_{7,\infty}(X) &= X^2 + (b\omega + a)X + \omega\\
g_{10,\infty}(X) &= X + \omega + 1,\\
g_{11,\infty}(X) &= X^2 + (-b\omega + (a - b))X - (\omega + 1).
\end{aligned} \tag{3}$$

for some $a \in \mathcal{O}_2$ where $b = -a - 1$. Here $g_{s,\infty}[X] \in \mathcal{O}_4[\omega]$ denotes the q-adic lift of $g_s[X]$. Plugging these lifts back to the factorization

$$X^{15} - 1 = (X - 1)\prod_s g_{s,\infty}(X) \tag{4}$$

in $\mathcal{O}_4[X]$ and expanding the product, we can obtain that the equality

$$\begin{aligned}
X^{15} - 1 =& X^{15} - 3(2 + 3a + 3a^2)X^{12} + (2 + 3a + 3a^2)^2(5 + 3a + 3a^2)X^9\\
&- (2 + 3a + 3a^2)^2(5 + 3a + 3a^2)X^6 + 3(2 + 3a + 3a^2)X^3 - 1.
\end{aligned}$$

Hence (4) holds if and only if $a \in \mathcal{O}_2$ satisfies

$$3a^2 + 3a + 2 = 0. \tag{5}$$

Notice that $b = -a - 1$ is also a solution of (5). Recall that $c \in \mathcal{O}_2$ has a square root if and only if $c \equiv 1 \pmod 8$. See [10] for detail. Since $-15 \equiv 1 \pmod 8$, we obtain two solutions for a as follows:

$$a = \frac{-3 \pm \sqrt{-15}}{6}. \tag{6}$$

Consequently, we have obtained the 4-adic liftings of $g_s(X)$ given by (3) with one of these a. Notice that replacing a with $-a-1$ gives the same list of factors.

Of course, solutions of (5) mod 2^e give $g_{s,e}(X)$ by the factorization given by (3). For an example, we get $a = 6, -7$ by solving (5) modulo 2^5 and it gives the factorization over $GR(2^5, 2)$.

3.2. Cyclic codes of length 17. Now we will consider cyclic codes over $\mathbb{F}_4$ of length 17. The cyclotomic cosets mod $n = 17$ over $\mathbb{F}_4$ are

$$\begin{aligned} &C_0 = \{0\}, \quad C_1 = \{1, 4, 16, 13\}, \quad C_2 = \{2, 8, 15, 9\}, \\ &C_3 = \{3, 12, 14, 5\}, \quad C_6 = \{6, 7, 11, 10\}. \end{aligned}$$

Hence $X^{17} - 1$ splits into linear factors over $\mathbb{F}_{4^4} = \mathbb{F}_2[\omega_4]$, where ω_4 is a primitive root of $f = X^8 + X^4 + X^3 + X^2 + 1 \in \mathbb{F}_2[X]$ of multiplicative order $4^4 - 1 = 255$. The subfield $\mathbb{F}_4$ consists of $\{0, 1, \omega, \omega^2\}$, where

$$\omega = {\omega_4}^{255/3} = {\omega_4}^7 + {\omega_4}^6 + {\omega_4}^4 + {\omega_4}^2 + \omega_4. \tag{7}$$

Let $\alpha \in \mathbb{F}_{4^4}$ be any primitive 17th root of unity. We may take $\alpha = \omega_4^{15}$. Now $X^{17} - 1$ factors over $\mathbb{F}_4$ as

$$X^{17} - 1 = (X - 1) g_1(X) g_2(X) g_3(X) g_6(X).$$

For $s = 1, 2, 3, 6$, let

$$\lambda_s = \sum_{i \in C_s} \alpha^i.$$

Using only the fact that α is a primitive 17th root of unity, we can show that the following formal identities hold:

$$\begin{aligned} g_1(X) &= X^4 - \lambda_1 X^3 + (\lambda_3 + 2) X^2 - \lambda_1 X + 1, \\ g_2(X) &= X^4 - \lambda_2 X^3 + (\lambda_6 + 2) X^2 - \lambda_2 X + 1, \\ g_3(X) &= X^4 - \lambda_3 X^3 + (\lambda_2 + 2) X^2 - \lambda_3 X + 1, \\ g_6(X) &= X^4 - \lambda_6 X^3 + (\lambda_1 + 2) X^2 - \lambda_6 X + 1. \end{aligned} \tag{8}$$

Let

$$\sigma_1 = \lambda_1 + \lambda_2, \quad \sigma_2 = \lambda_3 + \lambda_6.$$

Then σ_1 and σ_2 satisfy the identity

$$\sigma^2 + \sigma - 4 = 0. \tag{9}$$

Furthermore, we have the formal identities

$$\begin{aligned} g_1(X)g_2(X) &= X^8 - \sigma_1 X^7 + (3+\sigma_2)X^6 + (4+\sigma_2)X^5 + (3+2\sigma_2)X^4 \\ &\quad + (4+\sigma_2)X^3 + (3+\sigma_2)X^2 - \sigma_1 X + 1, \\ g_3(X)g_6(X) &= X^8 - \sigma_2 X^7 + (3+\sigma_1)X^6 + (4+\sigma_1)X^5 + (3+2\sigma_1)X^4 \\ &\quad + (4+\sigma_1)X^3 + (3+\sigma_1)X^2 - \sigma_2 X + 1. \end{aligned}$$

From these identities, we can show that the identity

$$X^{17} - 1 = (X-1)\prod_s g_{s,\infty}(X)$$

holds if and only if

$$\begin{aligned} \sigma_1 + \sigma_2 + 1 &= 0, \\ \sigma_1^2 + \sigma_1 - 4 &= 0. \end{aligned} \tag{10}$$

Note that (10) implies that $\sigma_2^2 + \sigma_2 - 4 = 0$, too.

Finally, one can show that the following formal identities also hold:

$$\begin{aligned} \lambda_1^2 &= \lambda_2 + 2\lambda_3 + 4, \quad & \lambda_2^2 &= \lambda_1 + 2\lambda_6 + 4, \\ \lambda_3^2 &= \lambda_6 + 2\lambda_2 + 4, \quad & \lambda_6^2 &= \lambda_3 + 2\lambda_1 + 4. \end{aligned} \tag{11}$$

Let $\sigma_1 = a\omega + b$. Then (10) implies that

$$\begin{aligned} a(1-a+2b) &= 0, \\ -4 - a^2 + b + b^2 &= 0. \end{aligned} \tag{12}$$

Let us go back to the case over $\mathbb{F}_4$. If $a \neq 0$, then $a = 1 + 2b$ and thus $3b^2 + 3b + 5 = 0$, which has no root b modulo 2 and hence for all 2^e. Hence we must have $a = 0$. Let $\lambda_i = a_i\omega + b_i$ for $i = 1, 2, 3, 6$. Then $a = 0$ means that

$$a_2 = -a_1, \quad a_6 = -a_3.$$

Now $\lambda_1 = \omega_4^{15} + \omega_4^{60} + \omega_4^{240} + \omega_4^{195}$. By the division algorithm over $\mathbb{F}_4$,

$$X^{15} + X^{60} + X^{240} + X^{195} \equiv X^7 + X^6 + X^4 + X^2 + X + 1 \pmod{f}.$$

This implies that $\lambda_1 = \omega + 1$ by (7). Similarly,

$$\lambda_2 = \omega, \quad \lambda_3 = 1, \quad \lambda_6 = 1.$$

Consequently, we have obtained the factorization of $X^{17} - 1$ over $\mathbb{F}_4$ given by (8).

We will lift $g_s(X)$ to $g_{s,e}(X) \in GR(2^e, 2)[X]$ for all $e = 2, 3, \cdots, \infty$ such that

$$X^{17} - 1 = (X - 1) \prod_s g_{s,e}(X).$$

Again, we can find $g_{s,e}$ for small e's by using MAGMA. For example, we list $g_{s,5}(X)$ over $GR(32, 2)$:

$$\begin{aligned} g_{1,5}(X) &= X^4 - (-\omega + 5)X^3 + (-6\omega - 7)X^2 - (-\omega + 5)X + 1, \\ g_{2,5}(X) &= X^4 - (\omega + 6)X^3 + (6\omega - 1)X^2 - (\omega + 6)X + 1, \\ g_{3,5}(X) &= X^4 - (-6\omega - 9)X^3 + (\omega + 8)X^2 - (-6\omega + 7)X + 1, \\ g_{6,5}(X) &= X^4 - (6\omega - 3)X^3 + (-\omega + 7)X^2 - (6\omega - 3)X + 1. \end{aligned} \tag{13}$$

From these lifts for small e's we conjecture that the q-adic lifts $g_{s,\infty}[X] \in \mathcal{O}_4[\omega]$ of $g_s[X]$ have the forms as in (8), this time with $\lambda_i = a_i\omega + b_i$ for some $a_i, b_i \in \mathcal{O}_2$ such that

$$a_1 = b_1 - b_2,\ a_2 = b_2 - b_1,\ a_3 = b_3 - b_6,\ a_6 = b_6 - b_3. \tag{14}$$

Moreover, (9) implies that $b_1 + b_2$ and $b_3 + b_6$ are roots of $x^2 + x - 4 = 0$, equivalently

$$\begin{aligned} (b_1 + b_2)^2 + (b_1 + b_2) - 4 &= 0, \\ b_1 + b_2 + b_3 + b_6 &= -1, \end{aligned} \tag{15}$$

and the first equation $\lambda_1^2 = \lambda_2 + 2\lambda_3 + 4$ of (11) implies

$$\begin{aligned} 4 + b_2 - 2b_1b_2 + b_2^2 + 2b_6 &= 0, \\ 2 + b_1 - b_1^2 + 3b_2 + b_2^2 + 4b_6 &= 0. \end{aligned} \tag{16}$$

Equations (15) and (16) implies that

$$\begin{aligned} (b_1 + b_2)^2 + (b_1 + b_2) - 4 &= 0, \\ 3b_1b_2 + (b_1 + b_2) - 5 &= 0. \end{aligned} \tag{17}$$

These equations also hold for b_3 and b_6 instead of b_1 and b_2.

The equation (13) shows that

$$b_1 \equiv b_3 \equiv b_6 \equiv 1,\ b_2 \equiv 0 \pmod 2 \tag{18}$$

Let κ, μ be two roots of $x^2 + x - 4 = 0$ in $\mathcal{O}_4$ such that $\kappa \equiv 1 \pmod 2$ and $\mu \equiv 0 \pmod 2$. Then $b_1 + b_2 = \kappa$ and $b_3 + b_6 = \mu$. By the second equation in (17), we then have

$$3b_1^2 - 3\kappa b_1 + (5-\kappa) = 0, \tag{19}$$

$$3b_3^2 - 3\mu b_3 + (5-\mu) = 0 \tag{20}$$

First, b_1 and b_2 are roots of the polynomial

$$f_1(x) = 3x^2 - 3\kappa x + (5-\kappa). \tag{21}$$

Since $f_1'(x) = 6x - 3\kappa \neq 0$ for odd κ, solving (21) modulo 2^e always gives exactly two solutions modulo 2^e. The solutions b_1, b_2 in $\mathcal{O}_2$ are given by

$$b_1, b_2 = \frac{3\kappa \pm \sqrt{9\kappa^2 + 12\kappa - 60}}{6}. \tag{22}$$

Next, to solve for b_3 and b_6, let $\mu = 2\mu_2$. The equation for b_3, b_6 from (20) is given by

$$3(x-\mu_2)^2 - (3\mu_2^2 + 2\mu_2 - 5) = 0. \tag{23}$$

Hence solutions b_3, b_6 in $\mathcal{O}_2$ are given by

$$b_3, b_6 = \mu_2 \pm \sqrt{\frac{3\mu_2^2 + 2\mu_2 - 5}{3}}. \tag{24}$$

More detailed explanation is need to find b_3, b_6. Let $M = (3\mu_2^2 + 2\mu_2 - 5)/3$. The equation (20) has solutions $\kappa \equiv 11$ and $\mu \equiv 4 \bmod 16$, hence $\mu_2 \equiv 2 \pmod 8$ and $3\mu_2^2 + 2\mu_2 - 5 \equiv 3 \pmod 8$. Hence $M \equiv 1 \pmod 8$, which implies that there exists $m \in \mathcal{O}_2$ such that $m^2 = M$ and then $x = \mu_2 \pm m$ are solutions for b_3, b_6 in (23). To find m, we need to find a root of $f_3(x) = x^2 - M = 0$. Since $f_3'(1) \equiv 0 \pmod 2$, we cannot use Hensel's lemma to find the roots. But, after the transform $\hat{m} = (m+1)/2$, $\hat{m}$ becomes a root of

$$y^2 - y - (M-1)/4 = 0. \tag{25}$$

Now we can use the Hensel's lemma to solve it modulo any 2^e since $2y + 1 \not\equiv 0 \pmod 2$.

As a final example, let us use our results to find the factorization of $X^{17} - 1$ over $GR(2^9, 2)$. By solving $x^2 + x - 4 \equiv 0 \pmod{2^9}$, we obtain $\kappa = 139$ and $\mu = 372$. We then solve the equation (21) modulo 2^9 to get $b_1 = 166, b_2 = 485$.

To solve for b_3, b_6, we need to be careful with μ_2. Note that

$$\mu = 2 + a_2 2^2 + \cdots + a_e 2^e + \cdots = 2(1 + a_2 2^1 + \cdots + a_e 2^{e-1} + \cdots)$$

in $\mathcal{O}_2$ so that $\mu_2 = 1 + a_2 2^1 + \cdots + a_e 2^{e-1} + \cdots$. To get $\mu_2 \bmod 2^e$, we thus need to get $\mu \bmod 2^{e+1}$. Solving $x^2 + x - 4 \equiv 0 \pmod{2^{10}}$, we get $\mu = 884$ and $\mu_2 = 442$. Then $M \equiv 73 \pmod{2^9}$ and $(M-1)/4 = 18$.

We now solve $y^2 - y - 18 \equiv 0 \pmod{2^9}$ to get $\hat{m} = 79, 434$ and then $m = 2\hat{m} - 1 = 157, 355$. Finally, $b_3, b_6 = \mu_2 + m = 87, 285$. By (8), we obtain the factorization

$$
\begin{aligned}
g_{1,9} &= X^4 - (193\omega + 166)X^3 + (198\omega + 287)X^2 - (193\omega + 166)X + 1 \\
g_{2,9} &= X^4 - (-193\omega + 485)X^3 + (-198\omega + 89)X^2 - (-193\omega + 485)X + 1 \\
g_{3,9} &= X^4 - (-198\omega + 87)X^3 + (193\omega + 168)X^2 - (-198\omega + 87)X + 1 \\
g_{6,9} &= X^4 - (198\omega + 285)X^3 + (-193\omega + 487)X^2 - (198\omega + 285)X + 1
\end{aligned}
$$

Notice that interchanging b_1, b_2 and b_3, b_6 gives the same factorization.

3.3. Cyclic codes of length 19. Finally let us consider cyclic codes of length 19. The cyclotomic cosets mod $n = 19$ are $C_0 = \{0\}$ together with

$$C_1 = \{1, 4, 16, 7, 9, 17, 11, 6, 5\}, \quad C_2 = \{2, 8, 13, 14, 18, 15, 3, 12, 10\}.$$

Hence $X^{19} - 1$ splits into linear factors over $\mathbb{F}_{4^9} = \mathbb{F}_2[\omega_9]$, where ω_9 is a primitive root of $f = X^{18} + X^{12} + X^{10} + X + 1$. Let $\alpha \in \mathbb{F}_{4^9}$ be any primitive 19th root of unity. Now $X^{19} - 1$ factors over $\mathbb{F}_4$ as

$$X^{19} - 1 = (X - 1)g_1(X)g_2(X)$$

where $g_s(X) = \prod_{i \in C_s}(X - \alpha^i)$. For $s = 1, 2$, let

$$\lambda_s = \sum_{i \in C_s} \alpha^i \in \mathcal{O}_4,$$

where $\lambda_1 + \lambda_2 + 1 = 0$. Using the fact that α is a primitive 19th root of unity, we obtain formal identities

$$
\begin{aligned}
g_1(X) =& X^9 - \lambda_1 X^8 - 2X^7 + (\lambda_1 + 2)X^6 - (\lambda_1 - 2)X^5 \\
& - (\lambda_1 + 3)X^4 + (\lambda_1 - 1)X^3 + 2X^2 + \lambda_2 X - 1, \\
g_2(X) =& X^9 - \lambda_2 X^8 - 2X^7 + (\lambda_2 + 2)X^6 - (\lambda_2 - 2)X^5 \\
& - (\lambda_2 + 3)X^4 + (\lambda_2 - 1)X^3 + 2X^2 + \lambda_1 X - 1
\end{aligned}
\tag{26}
$$

It is easy to check that λ_1 and λ_2 satisfy the equation

$$x^2 + x + 5 = 0. \tag{27}$$

Solutions of this give the complete factorization of $X^{19}-1$ over $\mathcal{O}_4$. To obtain these solutions concretely, let $\lambda_1 = a\omega + b$ with $a, b \in \mathcal{O}_2$. Then (27) is equivalent to

$$\begin{aligned} b^2 + b - a^2 + 5 &= 0 \\ a(1 - a + 2b) &= 0 \end{aligned} \tag{28}$$

If $a = 0$, then $b^2 + b + 5 = 0$, which is impossible mod 2. Thus $a = 1 + 2b$ and (28) is equivalent to

$$\begin{aligned} 3b^2 + 3b - 4 &= 0. \\ a &= 1 + 2b \end{aligned} \tag{29}$$

This equations give $b = (-3 \pm \sqrt{57})/6 \in \mathcal{O}_2$ and $a = 1 + 2b$ accordingly. Consequently we have obtained the factorization of $X^{19}-1$ over $\mathcal{O}_4$.

For the finite ring $GR(2^5, 2)$, we can solve the equation (29) mod 2^5 and obtain $b = 3, 28$ and then $a = 7, 25$. It gives the factorization as in (26) with $\lambda_1 = 7\omega + 3$ and $\lambda_2 = -7\omega + 28$.

References

[1] A.R.Calderbank, N.J.A. Sloane, *Modular and p-adic cyclic codes*, Des. Codes. Cryptogr. **6** (1995), 21–35.

[2] S.T. Dougherty, S.Y. Kim and Y.H. Park, *Lifted codes and their weight enumerators*, Discrete Math. **305** (2005), 123–135.

[3] S.T. Dougherty and Y.H. Park, *Codes over the p-adic integers*, Des. Codes. Cryptogr. **39** (2006), 65–80.

[4] F. Q. Gouvêa, *p-adic numbers. An introduction*, Springer, 2003.

[5] W.C. Huffman and V. Pless, *Fundamentals of error-correcting codes*, Cambridge, 2003.

[6] Wieb Bosma, John Cannon, and Catherine Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265. `http://magma.maths.usyd.edu.au/calc/`

[7] F.J. MacWilliams and N.J.A. Sloane, *The theory of error-correcting codes*, North-Holland, Amsterdam, 1977.

[8] Y.H. Park, *Modular independence and generator matrices for codes over $\mathbb{Z}_m$*, Des. Codes. Cryptogr. 50 (2009) 147–162

[9] Y.H. Park, *The q-adic litfings of codes over finite fields*, Korean J. Math. **26** (2018), 537–544

[10] J.-P. Serre, *Course in arithmetic*, Springer, 1973

Young Ho Park
Department of Mathematics
Kangwon National University
Chun Cheon 24341, Korea
E-mail: yhpark@kangwon.ac.kr