Cyclotomic numbers and primitive idempotents in the ring $\text{GF}(q)[x]/(x^{p^n} - 1)$

Anuradha Sharma,1 Gurmeet K. Bakshi, V.C. Dumir, and Madhu Raka*

Department of Mathematics, Centre for Advanced Study in Mathematics, Panjab University, Chandigarh 160014, India

Received 26 June 2003; revised 20 January 2004

Communicated by Vera Pless

Abstract

Let $q$ be an odd prime power and $p$ be an odd prime with $\gcd(p, q) = 1$. Let order of $q$ modulo $p$ be $f$, $\gcd(p-1, q) = 1$ and $q^f = 1 + p\lambda$. Here expressions for all the primitive idempotents in the ring $R_{p^n} = \text{GF}(q)[x]/(x^{p^n} - 1)$, for any positive integer $n$, are obtained in terms of cyclotomic numbers, provided $p$ does not divide $\lambda$ if $n \geq 2$. The dimension, generating polynomials and minimum distances of minimal cyclic codes of length $p^n$ over $\text{GF}(q)$ are also discussed.

© 2004 Elsevier Inc. All rights reserved.

Keywords: Cyclic codes; Cyclotomic cosets; Idempotents; Periods

1. Introduction

Let $\text{GF}(q)$ be a field of prime power order $q$, $q$ odd. Let $m \geq 1$ be an integer with $\gcd(q, m) = 1$. Let $R_m = \text{GF}(q)[x]/(x^m - 1)$. A cyclic code of length $m$ over $\text{GF}(q)$ is an ideal in the ring $R_m$. The set $\{0, 1, \ldots, m - 1\}$ is divided into disjoint cyclotomic cosets $C_s$, $0 \leq s \leq m - 1$, given by $C_s = \{s, sq, sq^2, \ldots, sq^{m-1}\}$ modulo $m$, where $m_s$ is the smallest positive integer such that $sq^{m_s} \equiv s \pmod{m}$. If $\alpha$ denotes a primitive $m$th root of unity in some extension field of $\text{GF}(q)$, then the polynomial

*Corresponding author.
E-mail address: mraka@pu.ac.in (M. Raka).

1 Research supported by N.B.H.M., India is gratefully acknowledged.
\(M^{(s)}(x) = \prod_{i=0}^{l} (x - \lambda^i)\) is the minimal polynomial of \(\lambda^i\) over \(GF(p^n)\) and the ideal \(M_s\) generated by \(\lambda^{m-1}\) is a minimal ideal in \(R_m\) (For reference see [12] and Chapter 8 of [8]). Every cyclic code of length \(m\) over \(GF(q)\) has a unique generator \(e(x)\) which is also an idempotent, i.e. \((e(x))^2 = e(x)\). The generator idempotent of the minimal ideal \(M_s\) is called the primitive idempotent and is denoted by \(\theta_s(x)\). It is known that

\[
\theta_s(x^j) = \begin{cases} 
1 & \text{if } j \in C_s, \\
0 & \text{if } j \notin C_s.
\end{cases}
\]

(1)

Any \(q\)-ary cyclic code of length \(m\) is a direct sum of the minimal ideals, generated by the primitive idempotents in \(R_m\). Thus the problem is to determine the primitive idempotents.

Construction of binary idempotents from the cyclotomic cosets is easy. In general, however, as stated by Pless [11, Section 3, p. 95], “we do not have much information about the codes generated. Only in special situations do we know the dimension.”

We consider non-binary cyclic codes only, i.e. we take \(q\) to be always odd. Berman [1, p. 22] gave explicit expression (without proof) for all the primitive idempotents in \(R_{p^n}\), where \(p, q\) are odd primes and \(q\) a primitive root modulo \(p^n\); Arora and Pruthi [9] verified it. Pruthi and Arora [10] also obtained all the primitive idempotents in \(R_{2p^n}\), where \(p\) is an odd prime and \(q\) a primitive root modulo \(2p^n\).

In a previous paper [4], Bakshi and Raka have derived all the primitive idempotents in the ring \(R_{p^n\ell}\), where \(p, \ell\) are distinct odd primes, \(q\) a primitive root modulo \(p^n\) and also modulo \(\ell\), with \(\gcd(\phi(p^n), \phi(\ell)) = 1\). Bakshi and Raka [3] obtained all the primitive idempotents in \(R_{2m, m \geq 3}\), when \(q \equiv 3\) or \(5 \pmod{8}\). Later the conditions on \(q\) were dropped and for all odd prime power \(q\), Bakshi et al. [2] derived all the primitive idempotents in \(R_{2m, m \geq 3}\).

In this paper, we generalize the result of Berman [1]. We take \(q\) to be an odd prime power, not necessarily a primitive root mod \(p^n\), where \(p\) is an odd prime, \(\gcd(p, q) = 1\). Let order of \(q\) modulo \(p\) be \(f\) and \(q^f = 1 + p\lambda\). Further suppose that \(p\) does not divide \(\lambda\), if \(n \geq 2\). Let \(\gcd(e, q) = 1\), where \(p = 1 + ef\). We give an algorithm to determine all the primitive idempotents in the ring \(R_{p^n} = GF(q)[x]/(x^{p^n} - 1)\), some of whose coefficients are eigenvalues of a special matrix \(\mathcal{A}\) (see Theorem 3, Section 4). When \(q\) is a primitive root mod \(p^n\), then \(f = p - 1\) and the result of Berman [1] follows as a corollary (see Corollary 2). In Corollary 3, we obtain all the primitive idempotents when \(e = 2\). The primitive idempotents of the quadratic residue codes mod \(p\) (see [8, Theorem 4, Chapter 16]) follow as a special case from Corollary 3. In Section 2, we obtain all the cyclotomic cosets modulo \(p^n\) (see Theorem 1). In Section 3, cyclotomic numbers and periods are defined and it is proved that the periods are eigenvalues of a special matrix \(\mathcal{A}\), occurring in a specific order (see Theorem 2). We also discuss, in Section 5, the dimension, generating polynomials and minimum distances of minimal cyclic codes of length \(p^n\). In Section 6, we give examples of all the ternary minimal cyclic codes of length 23 (here \(e = 2\)) and all the ternary and 5-ary minimal cyclic codes of length 13 (here \(e = 4\) and 3, respectively).
In another paper, we will generalize the result of Pruthi and Arora [10] and derive all the primitive idempotents in the ring \( R_{2p^n} \), where \( q \) is any odd prime power, not necessarily a primitive root mod \( 2p^n \), \( p \) being an odd prime.

2. Cyclotomic cosets modulo \( p^n \)

Throughout this paper, we assume that \( p \) is an odd prime, \( n \) is a positive integer, \( q \) is an odd prime power, \( \gcd(p, q) = 1 \). Let order of \( q \) modulo \( p \) be \( f = \frac{p-1}{e} \), where \( e \) is a positive integer and let \( f' = 1 + p\lambda \). Further suppose that \( p \) does not divide \( \lambda \), if \( n \geq 2 \). Let \( O_m(q) \) denote the order of \( q \) modulo \( m \). With these assumptions, we have

**Lemma 1.** \( O_{p^n}(q) = fp^{n-1} \) for all \( n \geq 1 \).

**Proof.** First note that for any integer \( r \geq 1 \),

\[
q^{f' r} = 1 + p^{r+1} \lambda_r,
\]

(2)

where \( p \) does not divide \( \lambda_r \). Let \( O_{p^n}(q) = t_n \). Since from (2), for \( r = n - 1 \), we have \( q^{f' p^{n-1}} \equiv 1 \pmod{p^n} \), so \( t_n \) divides \( fp^{n-1} \). Also \( q^n \equiv 1 \pmod{p} \) and \( O_p(q) = f \); therefore \( f \) divides \( t_n \). Let \( t_n = fp^u \) for some \( u, 0 \leq u \leq n - 1 \). Now \( q^n = q^{fp^u} = 1 + p^{u+1} \lambda_u \equiv 1 \pmod{p^n} \) which gives \( p^{u+1} \equiv 0 \pmod{p^n} \) as \( p \) does not divide \( \lambda_u \) which implies \( n \leq (u + 1) \). Hence \( u = n - 1 \) and so \( t_n = fp^{n-1} \). □

**Lemma 2.** Let \( g \) be a primitive root mod \( p \) such that \( \gcd\left(\frac{p^n-1}{p}, p\right) = 1 \), then \( g \) is a primitive root mod \( p^n \) also for all integers \( n \geq 1 \).

**Proof.** Let \( g^{p^n-1} = 1 + p\mu \), where \( p \) does not divide \( \mu \). Then working as in Lemma 1 with \( q \) replaced by \( g \) and with \( f = p - 1 \), we find that \( O_{p^n}(g) = \phi(p^n) \) for all \( n \geq 1 \). So \( g \) is a primitive root mod \( p^n \) for all \( n \geq 1 \). □

**Remark 1.** On replacing \( g \) by \( g + p \) (if necessary), we can always ensure that \( \gcd\left(\frac{p^n-1}{p}, p\right) = 1 \), so that there always exists a \( g \), which is a primitive root mod \( p^n \), for all \( n \geq 1 \).

**Theorem 1.** For each integer \( n \geq 1 \), there are \( (en + 1) \) distinct \( q \)-cyclotomic cosets mod \( p^n \), given by

\[
C_0 = \{0\},
\]

\[
C_{p^{j}g^{k}} = \{p^{j}g^{k}, p^{j}g^{k}q, p^{j}g^{k}q^{2}, \ldots, p^{j}g^{k}q^{p^{n-j+1}-1}\},
\]

for \( 0 \leq j \leq n - 1 \) and \( 0 \leq k \leq e - 1 \), where \( g \) is a primitive root mod \( p^n \).
Proof. The cosets $C_{p^{j}q^{k}}$, $0 \leq j \leq n - 1$ and $0 \leq k \leq e - 1$ are distinct mod $p^{n}$. For if there exists some $j, j', k, k', u, u'$ with $0 \leq j \leq j' \leq n - 1$, $0 \leq k, k' \leq e - 1$ and $0 \leq u \leq fp^{n-j-1} - 1$, $0 \leq u' \leq fp^{n-j'-1} - 1$ such that

$$p^{j}g^{k}q^{u} \equiv p^{j'}g^{k'}q^{u'} \pmod{p^{n}},$$

then

$$p^{j-j'}g^{k-k'}q^{u-u'} \equiv 1 \pmod{p^{n-j}}.$$  

As $p^{j-j'}$ divides $p^{n-j}$, we must have $p^{j-j'}|1$ which is possible if and only if $j = j'$. Therefore $g^{k-k'}q^{u-u'} \equiv 1 \pmod{p^{n-j}}$, which implies

$$g^{(k-k)(fp^{n-j-1})}q^{u-u}(fp^{n-j-1}) \equiv 1 \pmod{p^{n-j}}.$$  

By Lemma 1, $O_{p^{n-j}}(q) = fp^{n-j-1}$, so we get

$$g^{(k-k)(fp^{n-j-1})} \equiv 1 \pmod{p^{n-j}}.$$  

But $g$ is a primitive root mod $p^{n-j}$, so $e$ must divide $k' - k$. Also $0 \leq |k' - k| \leq e - 1$, so we must have $k' = k$. Thus $q^{u-u'} \equiv 1 \pmod{p^{n-j}}$ which implies that $fp^{n-j-1}$ divides $u - u'$. But $0 \leq |u - u'| \leq fp^{n-j-1} - 1$, so we must have $u' = u$. Hence all these cyclotomic cosets are disjoint mod $p^{n}$. Further these are all the cyclotomic cosets as

$$|C_{0}| = \sum_{j=0}^{n-1} \sum_{k=0}^{e-1} |C_{p^{j}q^{k}}| = 1 + \sum_{j=0}^{n-1} \sum_{k=0}^{e-1} fp^{n-j-1} = 1 + \sum_{j=0}^{n-1} \phi(p^{n-j}) = p^{n}. \quad \square$$

Remark 2.

1. If $f$ is even, then $-1 \equiv q^{p^{n-1}f} / 2 \pmod{p^{n}}$. So $-1 \in C_{1}$.
2. If $f$ is odd, there exist some $u$, $0 \leq u \leq p^{n-1}f - 1$, such that $g^{u}q^{u} \equiv 1 \pmod{p^{n}}$. So $-1 \in C_{g^{u}}$

3. Cyclotomic numbers and periods

For the definition of cyclotomic numbers and some results involving these, we refer to the Part 1 of [13]. Let $g$ be a primitive root mod $p$ ($p$ an odd prime) and $p = 1 + ef$. The Reduced Residue System (RRS) mod $p$ given by $\{1, g, g^{2}, \ldots, g^{p-2}\}$ is divided into $e$ disjoint classes $C_{i}$, for $i = 0, 1, 2, \ldots, e - 1$, where

$$C_{i} = \{g^{es+i} : s = 0, 1, 2, \ldots, f - 1\}.$$  

Clearly $C_{i} = C_{i+m}$ for any integer $m$. As the odd prime power $q$ has order $f = p^{-1} \pmod{p}$, $q$ is an $e$th power residue mod $p$. Therefore $q \equiv g^{es} \pmod{p}$ for some $s$,
0 ≤ s ≤ f − 1. Thus the class $\hat{C}_i$ is equal to \{g^i, g^{i+q}, g^{i+q^2}, \ldots, g^{i+q^{f-1}}\} modulo p, for each $i$, 0 ≤ i ≤ e − 1. If n = 1, the class $\hat{C}_i$ is same as $C_g^i$, defined earlier.

**Definition 1.** For fixed $i$ and $j$, 0 ≤ i ≤ e − 1, 0 ≤ j ≤ e − 1, the cyclotomic number $A_{ij}$ is defined to be the number of solutions of the equation

\[ z_i + 1 = z_j, \]  
where $z_i \in \hat{C}_i$, $z_j \in \hat{C}_j$, i.e. $A_{ij}$ is the number of ordered pairs $(s, t)$, such that

\[ g^{es+i} + 1 = g^{et+j}, \quad 0 ≤ s, t ≤ f − 1. \]

**Definition 2.** The cyclotomic matrix is the $e \times e$ matrix $N$ whose $(i, j)$th entry is the cyclotomic number $A_{ij}$.

Lemmas 3–6, stated below, follow from Lemmas 3, 6, 7, 19 and 19' of [13, Part I].

**Lemma 3.**

(a) For any integers $m$ and $n$, $A_{ij} = A_{(i+me)(j+ne)}$.

(b) $A_{ij} = A_{(e−i)(j−i)}$.

(c) $A_{ij} = \begin{cases} A_{ji} & \text{if } f \text{ is even,} \\ A_{(j+\frac{e}{2})(i+\frac{e}{2})} & \text{if } f \text{ is odd.} \end{cases}$

(d) $\sum_{j=0}^{e-1} A_{ij} = f - v_i$, where $v_i = \begin{cases} 1 & \text{if } f \text{ is even and } i = 0, \\ 1 & \text{if } f \text{ is odd and } i = \frac{e}{2}, \\ 0 & \text{otherwise.} \end{cases}$

(e) $\sum_{i=0}^{e-1} A_{ij} = f - \mu_j$, where $\mu_j = \begin{cases} 1 & \text{if } j = 0 \\ 0 & \text{otherwise.} \end{cases}$

**Lemma 4.** When $e = 2$, the cyclotomic matrix $N$ is given by

(i) $N = \begin{bmatrix} f - 2 & f \\ \frac{2}{f} & \frac{2}{f} \end{bmatrix}$ if $f$ is even,

(ii) $N = \begin{bmatrix} f - 1 & f + 1 \\ \frac{2}{f - 1} & \frac{2}{f - 1} \end{bmatrix}$ if $f$ is odd.

**Lemma 5.** When $e = 3$, the cyclotomic matrix $N$ is given by

$N = \begin{bmatrix} A & B & C \\ B & C & D \\ C & D & B \end{bmatrix}$,
together with the relations

\[ 9A = p - 8 + c, \]
\[ 18B = 2p - 4 - c - 9d, \]
\[ 18C = 2p - 4 - c + 9d, \]
\[ 9D = p + 1 + c, \]

where \( 4p \equiv c^2 + 27d^2 \) (mod q) with \( c \equiv 1 \) (mod 3).

Lemma 6.

(i) When \( e = 4 \) and \( f \) is odd, the cyclotomic matrix \( \mathcal{N} \) is given by

\[
\mathcal{N} = \begin{bmatrix}
A & B & C & D \\
E & E & D & B \\
A & E & A & E \\
E & D & B & E
\end{bmatrix},
\]

together with the relations

\[ 16A = p - 7 + 2s, \]
\[ 16B = p + 1 + 2s - 8t, \]
\[ 16C = p + 1 - 6s, \]
\[ 16D = p + 1 + 2s + 8t, \]
\[ 16E = p - 3 - 2s. \]

(ii) If \( e = 4 \) and \( f \) is even, the cyclotomic matrix \( \mathcal{N} \) is given by

\[
\mathcal{N} = \begin{bmatrix}
A & B & C & D \\
B & D & E & E \\
C & E & C & E \\
D & E & E & B
\end{bmatrix},
\]

together with the relations

\[ 16A = p - 11 - 6s, \]
\[ 16B = p - 3 + 2s + 8t, \]
\[ 16C = p - 3 + 2s, \]
\[16D = p - 3 + 2s - 8t,\]
\[16E = p + 1 - 2s,\]

where \(p \equiv s^2 + 4t^2 \pmod{q}\), \(s \equiv 1 \pmod{4}\) is the proper representation of \(p\) if \(p \equiv 1 \pmod{4}\). (A representation \(p = x^2 + dy^2\) is said to be proper if \(\gcd(p, x) = 1\).

**Remark 3.**

(i) The sign of \(d\) in Lemma 5 and the sign of \(t\) in Lemma 6 are also uniquely determined. For this, see Katre and Rajwade [6,7].

(ii) The cyclotomic numbers are known for all values of \(e\) in terms of Jacobi sums. For reference, see Katre [5] and Paul Van Wamelen [14].

**Definition 3.** For \(0 \leq k \leq e - 1\), the period \(\eta_k\) is defined as

\[
\eta_k = \sum_{t=0}^{f-1} \beta^{tq^e} = \sum_{t=0}^{f-1} \beta^{te+k} = \sum_{j \in C_k} \beta^j, \tag{3}
\]

where \(\beta\) is a primitive \(p\)th root of unity in some extension field of \(GF(q)\).

The periods defined above are similar to the periods defined in [13, p. 38] with \(\alpha = 1\) except that our \(\beta\) is not a complex primitive \(p\)th root of unity, it is a primitive \(p\)th root of unity in \(GF(q')\).

The following result holds true for this \(\beta\) also; for a proof see Corollary to Lemmas 8 and 9 of [13, pp. 38–40].

**Lemma 7.**

(i) \(\eta_k = \eta_{k+me}\) for any integer \(m\).

(ii) \(\sum_{k=0}^{e-1} \eta_k = -1\).

(iii) \(\eta_i \eta_{i+k} = \sum_{h=0}^{e-1} A_{kh} \eta_{i+h} + f v_k\).

(iv) \(\sum_{j=0}^{e-1} \eta_j \eta_{j+k} = pv_k - f, \quad 0 \leq k \leq e - 1\),

where \(v_k\) is as defined in Lemma 3.

**Definition 4.** Let \(X = (x_0, x_1, x_2, \ldots, x_{e-1})\) be a vector over \(GF(q)\). For \(0 \leq k \leq e - 1\), we define \(\sigma^k(X)\) as the \(k\)th cyclic shift of \(X\) i.e.

\[\sigma^k(X) = (x_k, x_{k+1}, x_{k+2}, \ldots, x_{k-1}).\]

**Definition 5.** Let \(\mathcal{A} = (a_{ij}), 0 \leq i \leq e - 1, 0 \leq j \leq e - 1\) be any \(e \times e\) matrix over \(GF(q)\). Let \(X = (x_0, x_1, x_2, \ldots, x_{e-1})^T\) be an eigenvector of \(\mathcal{A}\), where \(^T\) stands for the
transpose of a matrix. We say that \( X \) has cyclic property if for each \( k, 0 \leq k \leq e - 1 \), \( \sigma^k(X) \) is also an eigenvector of \( \mathcal{A} \).

Let \( \mathcal{A} \) denote the \( e \times e \) matrix given by

\[
\begin{bmatrix}
A_{00} - f & A_{01} - f & A_{02} - f & \cdots & A_{0(e-1)} - f \\
A_{10} & A_{11} & A_{12} & \cdots & A_{1(e-1)} \\
A_{20} & A_{21} & A_{22} & \cdots & A_{2(e-1)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
A_{(e-1)0} & A_{(e-1)1} & A_{(e-1)2} & \cdots & A_{(e-1)(e-1)}
\end{bmatrix}
\]

if \( f \) is even

and is given by

\[
\begin{bmatrix}
A_{00} & A_{01} & A_{02} & \cdots & A_{0(e-1)} \\
A_{10} & A_{11} & A_{12} & \cdots & A_{1(e-1)} \\
A_{20} & A_{21} & A_{22} & \cdots & A_{2(e-1)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
A_{(\frac{e}{2})0} - f & A_{(\frac{e}{2})1} - f & A_{(\frac{e}{2})2} - f & \cdots & A_{(\frac{e}{2})(e-1)} - f \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
A_{(e-1)0} & A_{(e-1)1} & A_{(e-1)2} & \cdots & A_{(e-1)(e-1)}
\end{bmatrix}
\]

if \( f \) is odd,

where \( A_{ij} \)'s are the cyclotomic numbers defined in Definition 1. The matrix \( \mathcal{A} \) is obtained from the matrix \( \mathcal{N} \) by subtracting \( f \) from the first row, if \( f \) is even and from the \( (\frac{e}{2} + 1) \)th row, if \( f \) is odd.

**Theorem 2.** Let \( \gcd(e, q) = 1 \).

(i) The period \( \eta_i \) is an eigenvalue of the matrix \( \mathcal{A} \) with \( P_i = (\eta_i, \eta_{i+1}, \eta_{i+2}, \ldots, \eta_{i-1})^T \) as a corresponding eigenvector with first entry \( \eta_i \), for each \( i, 0 \leq i \leq e - 1 \).

(Thus the eigenvector \( P_i \), for each \( i \), has the cyclic property.)

(ii) The matrix \( P = (P_0 \ P_1 \ P_2 \ \cdots \ P_{e-1}) \) having the eigenvector \( P_i \) as its \((i + 1)\)th column is nonsingular, so that \( \eta_0, \eta_1, \eta_2, \ldots, \eta_{e-1} \) are all the eigenvalues of \( \mathcal{A} \), counted with multiplicity.

(iii) If \( X = (\rho_0, \rho_1, \rho_2, \ldots, \rho_{e-1})^T \) is another eigenvector of \( \mathcal{A} \) with cyclic property, then \( X = \alpha P_j \) for some \( j, 0 \leq j \leq e - 1 \) and for some scalar \( \alpha \in \text{GF}(q) \).

In addition, if \( \sum_{i=0}^{e-1} \rho_i = -1 \), then \( X = P_j \) for some \( j \).

**Proof.** (i) We prove the result when \( f \) is even. The case when \( f \) is odd, being similar, is left to the reader. By Lemma 7(iii), for any \( i, 0 \leq i \leq e - 1 \), we have

\[
\eta_i^2 = A_{00}\eta_i + A_{01}\eta_{i+1} + A_{02}\eta_{i+2} + \cdots + A_{0(e-1)}\eta_{i-1} + f
\]

\[
\eta_i\eta_{i+1} = A_{10}\eta_i + A_{11}\eta_{i+1} + A_{12}\eta_{i+2} + \cdots + A_{1(e-1)}\eta_{i-1}
\]
\[ \eta_i \eta_{i+2} = A_{20} \eta_i + A_{21} \eta_{i+1} + A_{22} \eta_{i+2} + \cdots + A_{2(e-1)} \eta_{i-1} \]
\[ \cdots \cdots \]
\[ \eta_i \eta_{i+e-1} = A_{(e-1)0} \eta_i + A_{(e-1)1} \eta_{i+1} + A_{(e-1)2} \eta_{i+2} + \cdots + A_{(e-1)(e-1)} \eta_{i-1}. \]

Using \( f = -f(\eta_0 + \eta_1 + \eta_2 + \cdots + \eta_{e-1}) \), \( \eta_{i+e-1} = \eta_{i-1} \) and rewriting, we get

\[ (A_{00} - f - \eta_i) \eta_i + (A_{01} - f) \eta_{i+1} + A_{02} \eta_{i+2} + \cdots + (A_{0(e-1)} - f) \eta_{i-1} = 0 \]
\[ A_{10} \eta_i + (A_{11} - \eta_i) \eta_{i+1} + A_{12} \eta_{i+2} + \cdots + A_{1(e-1)} \eta_{i-1} = 0 \]
\[ A_{20} \eta_i + A_{21} \eta_{i+1} + (A_{22} - \eta_i) \eta_{i+2} + \cdots + A_{2(e-1)} \eta_{i-1} = 0 \]
\[ \cdots \cdots \]
\[ A_{(e-1)0} \eta_i + A_{(e-1)1} \eta_{i+1} + A_{(e-1)2} \eta_{i+2} + \cdots + (A_{(e-1)(e-1)} - \eta_i) \eta_{i-1} = 0; \]

i.e.

\[
\begin{pmatrix}
\eta_i \\
\eta_{i+1} \\
\eta_{i+2} \\
\vdots \\
\eta_{i-1}
\end{pmatrix} = 0.
\]

Since \( P = (\eta_i; \eta_{i+1}; \eta_{i+2}; \ldots; \eta_{i-1})^T \) is a nonzero vector (because the sum \( \sum_{i=0}^{e-1} \eta_i = -1 \)), we see that \( \eta_i \) is an eigenvalue of \( \mathcal{A} \) with \( P_i \) as a corresponding eigenvector.

(ii) To show that \( P \) is nonsingular, it is enough to show that the matrix

\[
M = \begin{bmatrix}
\eta_0 & \eta_1 & \eta_2 & \cdots & \eta_{e-1} \\
\eta_{e-1} & \eta_0 & \eta_1 & \cdots & \eta_{e-2} \\
\eta_{e-2} & \eta_{e-1} & \eta_0 & \cdots & \eta_{e-3} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
\eta_1 & \eta_2 & \eta_3 & \cdots & \eta_0
\end{bmatrix}
\]

is nonsingular, as \( M \) is obtained from \( P \) by interchange of rows. Let

\[
V = \begin{bmatrix}
1 & 1 & 1 & \cdots & 1 \\
1 & \zeta & \zeta^2 & \cdots & \zeta^{e-1} \\
1 & \zeta^2 & \zeta^4 & \cdots & \zeta^{2(e-1)} \\
\vdots & \vdots & \vdots & \ddots & \vdots \\
1 & \zeta^{e-1} & \zeta^{2(e-1)} & \cdots & \zeta^{(e-1)(e-1)}
\end{bmatrix}
\]
be the Vandermonde matrix, where $\zeta$ is a primitive $e$th root of unity in an extension field of $GF(q)$. Then it is easy to see that

$$V^{-1}MV = \text{diag}(F(1), F(\zeta), F(\zeta^2), \ldots, F(\zeta^{e-1})),$$

where $F(x) = \eta_0 + \eta_1x + \eta_2x^2 + \cdots + \eta_{e-1}x^{e-1}$. Also

$$F(\zeta^m)F(\zeta^{-m}) = \left(\sum_{j=0}^{e-1} \zeta^{mj}\eta_j\right)\left(\sum_{k=0}^{e-1} \zeta^{-mk}\eta_k\right) = \left(\sum_{j=0}^{e-1} \zeta^{mj}\eta_j\right)\left(\sum_{k=0}^{e-1} \zeta^{-m(k+j)}\eta_{k+j}\right)$$

$$= \sum_{k=0}^{e-1} \zeta^{-mk} \sum_{j=0}^{e-1} \eta_j\eta_{j+k} = \sum_{k=0}^{e-1} \zeta^{-mk}(p\eta_k - f) \quad \text{(by Lemma 7(iv))}$$

$$= p \sum_{k=0}^{e-1} \zeta^{-mk}v_k = \begin{cases} 1 & \text{if } f \text{ is even,} \\ 0 & \text{if } f \text{ is odd.} \end{cases}$$

Therefore $F(\zeta^m) \neq 0$, for any $m$, which gives det $M = F(1)F(\zeta)F(\zeta^2)\cdots F(\zeta^{e-1}) \neq 0$. So $M$ and hence $P$ is nonsingular.

Now since $\mathcal{A}P_i = \eta_i P_i$, we have $\mathcal{A}P = \text{diag}(\eta_0, \eta_1, \eta_2, \ldots, \eta_{e-1}), P$, i.e.

$$P^{-1}\mathcal{A}P = \text{diag}(\eta_0, \eta_1, \eta_2, \ldots, \eta_{e-1}).$$

Similar matrices have the same eigenvalues, so $\eta_i$, $0 \leq i \leq e-1$ are all the eigenvalues of $\mathcal{A}$.

(iii) Suppose $X$ corresponds to the eigenvalue $\eta_k$, therefore $X \in W_k$ where $W_k$ is the eigenspace of $\eta_k$. Suppose $W_k$ is generated by eigenvectors $P_k_1$, $P_k_2$, $\ldots$, $P_k_i$ corresponding to eigenvalues $\eta_{k_1} = \eta_{k_2} = \eta_{k_3} = \cdots = \eta_{k_r}$. Let

$$X = x_1P_k_1 + x_2P_k_2 + \cdots + x_rP_k_r, \quad (4)$$

where $x_i \in GF(q)$.

We assert that exactly one of $x_i$'s is non-zero. For this, we will show that for any pair $(x_i, x_j)$, $1 \leq i, j \leq r$, $i \neq j$, at least one of $x_i, x_j$ is zero by taking a suitable cyclic shift of (4).

Without loss of generality, consider the pair $(x_1, x_2)$. Since $P_k_1$ and $P_k_2$ are distinct vectors, there exists some $t$ such that $\eta_{k_1+t} \neq \eta_{k_2+t}$. Taking $t$th cyclic shift of (4), we have

$$\sigma^t(X) = x_1\sigma^t(P_k_1) + x_2\sigma^t(P_k_2) + \cdots + x_r\sigma^t(P_k_r). \quad (5)$$

By parts (i) and (ii) of Theorem 2 and the given hypothesis, each of $\sigma^t(P_k_j)$, $1 \leq j \leq r$, and $\sigma^t(X)$ is also an eigenvector of the matrix $\mathcal{A}$. Also $\sigma^t(P_k_1)$ and $\sigma^t(P_k_2)$ are in different eigenspaces, say $W_{k_1+t}$ and $W_{k_2+t}$; as they correspond to distinct eigenvalues $\eta_{k_1+t}$ and $\eta_{k_2+t}$. We group the vectors on the right hand side of (5) according as they lie in $W_{k_1+t}$ or $W_{k_2+t}$ or in eigenspaces different from these two,
to get
\[
\sigma^i(X) = \left(\lambda_1\sigma^i(P_{k_1}) + \sum_i \lambda_i \sigma^i(P_{k_i})\right) + \left(\lambda_2\sigma^i(P_{k_2}) + \sum_j \lambda_j \sigma^i(P_{k_j})\right) + \left(\sum_r \lambda_r \sigma^i(P_{k_r})\right).
\]

Now the eigenvectors \(\sigma^i(P_{k_i}), 1 \leq i \leq \ell\) are linearly independent. So, we must have \(\lambda_2 = 0\) if \(\sigma^i(X) \in W_{k_1+\ell}\); \(\lambda_1 = 0\) if \(\sigma^i(X) \in W_{k_2+\ell}\); \(\lambda_1 = \lambda_2 = 0\) if \(\sigma^i(X)\) is not in \(W_{k_1+\ell} \cup W_{k_2+\ell}\). This proves our assertion for the pair \((\lambda_1, \lambda_2)\). Hence we must have \(X = \lambda_j P_{k_j}\) for some \(j, 1 \leq j \leq \ell\). Further if \(\sum_{i=0}^{e-1} \rho_i = -1\), then we must have \(\lambda_j = 1\) as \(\sum_{i=0}^{e-1} \eta_i = -1\).

**Corollary 1.** For each \(j, 0 \leq j \leq e - 1\), let \(\chi_j\) be the character defined on a group of reduced residue classes mod \(p\), by
\[
\chi_j(g^{ex+i}) = \zeta^{ij} \quad \text{for } 0 \leq i \leq e - 1, \ 0 \leq s \leq f - 1,
\]
where \(\zeta\) is a primitive \(e\)-th root of unity in an extension field of \(GF(q)\). Then the Gaussian sums \(\tau(\chi_j)\) (having values in a finite field) for \(0 \leq j \leq e - 1\) defined as
\[
\tau(\chi_j) = \sum_{x \in RRS \mod p} \chi_j(x) \beta^x = \sum_{i=0}^{e-1} \sum_{s=0}^{f-1} \chi_j(g^{ex+i}) \beta^{\rho^{ex+i}} = \sum_{i=0}^{e-1} \sum_{s=0}^{f-1} \beta^{\rho^{ex+i}}
\]
\[
= \sum_{i=0}^{e-1} \eta_i \zeta^i = \eta_0 + \eta_1 \zeta + \eta_2 \zeta^2 + \eta_{e-1} \zeta^{(e-1)} = F(\zeta^j)
\]
can be evaluated once the values of the periods \(\eta_0, \eta_1, \ldots, \eta_{e-1}\) are determined by Theorem 2.

**Lemma 8.**

(i) If \(e = 1\), the only eigenvalue \(\eta_0 = -1\).

(ii) If \(e = 2\), we can take \(\eta_0 = \frac{-1+\delta}{2}, \ \eta_1 = \frac{-1-\delta}{2}\), where \(\delta \in GF(q)\) is given by
\[
\delta^2 = \begin{cases} 
p & \text{if } p \equiv 1 \pmod{4}, 
-p & \text{if } p \equiv 3 \pmod{4}.
\end{cases}
\]

(iii) If \(e = 3\), the characteristic equation of the matrix \(\mathcal{A}\) is given by
\[
x^3 + x^2 - \left(\frac{p - 1}{3}\right)x - \left(\frac{p(c + 3) - 1}{27}\right) = 0,
\]
where \(c\) is as defined in Lemma 5.
(iv) If \( e = 4 \), the characteristic equation of the matrix \( \mathcal{A} \) is given by
\[
x^4 + x^3 - 3\left(\frac{p - 1}{8}\right)x^2 + \left(\frac{1 - 3p + 2ps}{16}\right)x + \left(\frac{1 - 6p + 8ps - 4ps^2 + p^2}{256}\right) = 0,
\]
if \( f \) is even and by
\[
x^4 + x^3 + \left(\frac{p + 3}{8}\right)x^2 + \left(\frac{1 + p + 2ps}{16}\right)x + \left(\frac{1 + 2p + 8ps - 4ps^2 + 9p^2}{256}\right) = 0,
\]
if \( f \) is odd; where \( s \) is as defined in Lemma 6.

Proof.
(i) This is trivial because \( A_{00} = p - 2 = f - 1 \) and \( \mathcal{A} = (A_{00} - f) = (-1) \).
(ii) By Lemma 4, the characteristic equation of the matrix \( \mathcal{A} \) is
\[
x^2 + x - \left(\frac{p - 1}{4}\right) = 0 \quad \text{if } p \equiv 1 \pmod{4},
\]
\[
x^2 + x + \left(\frac{p + 1}{4}\right) = 0 \quad \text{if } p \equiv 3 \pmod{4}.
\]
Solving this, we can take \( \eta_0 = -\frac{1 + \delta}{2}, \eta_1 = -\frac{1 - \delta}{2} \), where \( \delta^2 = p \) if \( p \equiv 1 \pmod{4} \), and \( \delta^2 = -p \) if \( p \equiv 3 \pmod{4} \).
Using Lemmas 5 and 6 and the definition of the matrix \( \mathcal{A} \), (iii) and (iv) are obtained after a simple calculation (with the help of Maple8).

4. Primitive idempotents in the ring \( R_{p^n} \)

Let \( z \) be a primitive \((p^n)\)th root of unity in the extension field \( GF(q^{p^n-1}f) \) of \( GF(q) \). For a fixed \( s \), define the polynomial
\[
\Omega_s(x) = \sum_{j \in C_{p^n-1}} x^j.
\]

4.1. An algorithm to compute primitive idempotents in the ring \( R_{p^n} \)

Step I: Find a primitive root \( g \mod p \) such that \( \gcd(g^{p^n-1}-1, p) = 1 \).
Step II: Evaluate all the \( e^2 \) cyclotomic numbers \( A_{ij} \), \( 0 \leq i, j \leq e - 1 \).
Step III: Find all the eigenvalues of matrix \( \mathcal{A} \).
Step IV: Fix an eigenvalue \( \rho_0 \) of \( \mathcal{A} \). Corresponding to \( \rho_0 \), find an eigenvector \( P_0 = (\rho_0, \rho_1, \rho_2, \ldots, \rho_{e-1}) \), whose first entry is \( \rho_0 \) and other entries \( \rho_i \), for \( 1 \leq i \leq e - 1 \), are the remaining eigenvalues of \( \mathcal{A} \) with \( \sum_{i=0}^{e-1} \rho_i = -1 \) and \( P_0 \) having cyclic property. (Such a \( P_0 \) exists uniquely by Theorem 2).
Step V: Compute the following polynomials over $GF(q)$, for $0 \leq j \leq n - 1$,

$$
\theta_0(x) = \frac{1}{p^n} (1 + x + x^2 + x^3 + \cdots + x^{p^n-1}),
$$

$$
\theta_{pj}(x) = \frac{f}{p^{j+1}} \sum_{i=0}^{p^n-1} x^i + \frac{1}{p^{j+1}} \{ \rho_0 \Omega_j(x) + \rho_1 \Omega_j(x^q) + \cdots + \rho_{e-1} \Omega_j(x^{q^{e-1}}) \},
$$

$$
\theta_{gpj}(x) = \frac{f}{p^{j+1}} \sum_{i=0}^{p^n-1} x^i + \frac{1}{p^{j+1}} \{ \rho_1 \Omega_j(x) + \rho_2 \Omega_j(x^{q}) + \cdots + \rho_0 \Omega_j(x^{q^{e-1}}) \},
$$

$$
\theta_{pj^{e-1}}(x) = \frac{f}{p^{j+1}} \sum_{i=0}^{p^n-1} x^i + \frac{1}{p^{j+1}} \{ \rho_{e-1} \Omega_j(x) + \rho_e \Omega_j(x^{q^{e-1}}) \}.
$$

Theorem 3. Let $p$ be an odd prime and $q$ be an odd prime power, with $\gcd(p, q) = 1$. Let order of $q$ modulo $p$ be $f$ and $q^f = 1 + p\lambda$. Further suppose that $p$ does not divide $\lambda$, if $n \geq 2$. Let $\gcd(e, q) = 1$, where $p = 1 + ef$. Then we can choose $\alpha$, a primitive $(p^n)$th root of unity, suitably, so that Step V of the above Algorithm gives all the $(en + 1)$ primitive idempotents in $R_{p^n}$.

To prove the Theorem, we need the following results:

**Lemma 9.** If $\alpha$ is a primitive $(p^n)$th root of unity, the primitive idempotent $\theta_s(x)$ corresponding to the cyclotomic coset $C_s$, is given by

$$
\theta_s(x) = \sum_{i=0}^{p^n-1} e_i^{(s)} x^i, \quad \text{where } e_i^{(s)} = \frac{1}{p^n} \sum_{j \in C_s} \alpha^{-ij}.
$$

This is Theorem 6, Chapter 8 of [8] generalized to nonbinary case.

**Lemma 10.** Let $\gcd(a, p) = 1$, $p = 1 + ef$.

(i) For any integer $k \geq 1$, $a$ is an eth power residue mod $p^k$ if and only if

$$
a^{p^{k-1}} \equiv 1 \pmod{p^k}.
$$

(ii) If $a$ is an eth power residue mod $p$, then $a + \mu p$, for any $\mu$, is an eth power residue mod $p^k$, for all $k \geq 1$.

(iii) The set

$$
S = \left\{ a + \mu p : a \text{ runs over eth power residues mod } p, \mu \text{ runs over Complete Residue System (CRS) mod } p^{k-1} \right\}
$$

consists of all the $fp^{k-1}$ incongruent eth power residues mod $p^k$. 
Proof. (i) Write \( a \equiv g^x \pmod{p^k} \) and \( x \equiv g^t \pmod{p^k} \). Then \( x^e \equiv a \pmod{p^k} \) has a solution in \( x \) if and only if \( g^{te} \equiv g^t \pmod{p^k} \) has a solution in \( t \). As \( g \) is a primitive root mod \( p^k \), this is so if and only if \( te \equiv s \pmod{\phi(p^k)} \) has a solution in \( t \) i.e. if and only if \( \gcd(e, \phi(p^k)) = e \) divides \( s \). If \( s = er \) for some \( r \), this is so if and only if \( a^{f_{p^k-1}} \equiv g^{f_{p^k-1}} \equiv 1 \pmod{p^k} \).

(ii) Write \( a^f = 1 + pt \) for some \( t \). Then

\[
(a + \mu p)^{f_{p^k-1}} \equiv a^{f_{p^k-1}} \equiv (1 + pt)^{f_{p^k-1}} \equiv 1 \pmod{p^k}
\]

and the result follows by Case(i).

(iii) It is obvious as \( a + \mu_1 p \equiv a + \mu_2 p \pmod{p^k} \) iff \( \mu_1 \equiv \mu_2 \pmod{p^{k-1}} \) and there are exactly \( f \) incongruent \( e \)th power residues mod \( p \).

\[\square\]

Lemma 11. Let \( \gamma \) be a primitive \( (p^k) \)th root of unity with \( k \geq 2 \). Then the sums

\[ S_i = \gamma^{g^i} + \gamma^{g^2} + \cdots + \gamma^{g^{f_{p^k-1}}} \]

have value equal to zero for every \( i, 0 \leq i \leq e - 1 \).

Proof. Since, for every \( j \), \( (q^j)^f \equiv 1 \pmod{p} \), \( q^j \) is an \( e \)th power residue mod \( p \) and hence, by Lemma 10(ii), an \( e \)th power residue mod \( p^k \). So the set \( \{1, q, q^2, \ldots, q^{f_{p^k-1}}\} \) consists of \( e \)th power residues mod \( p^k \). Their number being exactly \( f_{p^k-1} \), we see, using Lemma 10(iii), that modulo \( p^k \)

\[
\{1, q, q^2, \ldots, q^{f_{p^k-1}}\} = S = \left\{ a + \mu p : \begin{array}{c} a \text{ runs over } e \text{th power residues mod } p, \\ \mu \text{ runs over CRS mod } p^{k-1}. \end{array} \right\}
\]

Therefore

\[
S_i = \sum_{j=0}^{f_{p^k-1}-1} \gamma^{g^j} = \sum_a \sum_\mu \gamma^{g^j(a+\mu p)} = \sum_a \gamma^{g^a} \sum_\mu \zeta^\mu,
\]

where \( \zeta = \gamma^g \) is a primitive \( (p^{k-1}) \)th root of unity; \( a \) runs over \( e \)th power residues mod \( p \) and \( \mu \) runs over CRS mod \( p^{k-1} \). As \( k \geq 2 \), \( \zeta \neq 1 \), \( \zeta^{p^{k-1}} = 1 \), so we get

\[
\sum_\mu \zeta^\mu = 1 + \zeta + \zeta^2 + \cdots + \zeta^{f_{p^k-1}-1} = \frac{\zeta^{p^{k-1}} - 1}{\zeta - 1} = 0.
\]

Hence, from (6), we get that \( S_i = 0 \), for each \( i, 0 \leq i \leq e - 1 \). \[\square\]
Proof of Theorem 3. By Lemma 9,

$$\theta_0(x) = \sum_{i=0}^{p^n-1} e_i^{(0)} x^i,$$

where $$e_i^{(0)} = \frac{1}{p^n} \sum_{h \in C_0} \alpha^{-ih} = \frac{1}{p^n},$$

for every $$i$$, as $$C_0 = \{0\}$$. Thus

$$\theta_0(x) = \frac{1}{p^n} (1 + x + x^2 + x^3 + \cdots + x^{p^n-1}).$$

For any $$j$$, $$0 \leq j \leq n - 1$$, we have, by Lemma 9,

$$\theta_p(x) = \sum_{i=0}^{p^n-1} e_i^{(p')} x^i,$$

where $$e_i^{(p')} = \frac{1}{p^n} \sum_{h \in C_{p'}} \alpha^{-ip'q^{j}} = \frac{1}{p^n} \sum_{h=0}^{p^{n-j-1}f-1} \alpha^{-ip'q^{j}}.$$

As the value of $$e_i^{(p')}$$ remains same for all $$i$$ in a cyclotomic coset, we have

$$\theta_{p'}(x) = e_0^{(p')} + \sum_{r=0}^{e-1} \sum_{s=0}^{n-1} e_{i\gamma^r p'}^{(p')} \sum_{i \in C_{\gamma^r p'}} x^i.$$

Now

$$e_0^{(p')} = \frac{1}{p^n} \sum_{h=0}^{p^{n-j-1}f-1} \alpha^{-hp'q^{j}} = \frac{f}{p^{j+1}}.$$

If $$s \geq n - j$$,

$$e_{i\gamma^r p'}^{(p')} = \frac{1}{p^n} \sum_{h=0}^{p^{n-j-1}f-1} \alpha^{-ip'\gamma^r q^{j}} = \frac{f}{p^{j+1}}.$$

If $$0 \leq s \leq n - j - 1$$, then

$$e_{i\gamma^r p'}^{(p')} = \frac{1}{p^n} \sum_{h=0}^{p^{n-j-1}f-1} \gamma^r q^{j}, \quad (7)$$

where $$\gamma = \alpha^{-p'q^h}$$ is a primitive $$(p^{n-s-j})$$th root of unity.

Now $$\gamma^r q^{j} = \gamma^s q^{h}$$ if and only if $$q^{j} \equiv q^{h} \pmod{p^{n-s-j}}$$ if and only if $$h \equiv h' \pmod{fp^{n-s-j-1}}$$ because $$O_{p^{n-s-j}}(q) = fp^{n-s-j-1}$$.

Thus from (7), we get

$$e_{i\gamma^r p'}^{(p')} = \frac{1}{p^n} \sum_{h=0}^{p^{n-j-1}f-1} \gamma^r q^{j}, \quad (8)$$
If $k = n - s - j \geq 2$ i.e. if $0 \leq s \leq n - j - 2$, then the sum on the right hand side of (8) is $S_r$, which is zero by Lemma 11.

If $s = n - j - 1$, by (8), we have

$$\frac{\varepsilon_{p^j}(q)}{p^{j+1}} = \frac{1}{p^{j+1}} \sum_{h=0}^{f-1} p^h q^h = \frac{1}{p^{j+1}} \eta_r,$$

where $\beta = \gamma = x^{p^j-1}$ is a primitive $p$th root of unity and $\eta_r$ is the period as defined in Section 3. We choose $\alpha$ and hence $\beta$ suitably to have $\eta_r = p_r$. Therefore

$$\theta_{p^j\alpha}(x) = \frac{f}{p^{j+1}} + f \sum_{r=0}^{e-1} \sum_{s=n-j}^{n-1} \sum_{i \in C_{p^j\alpha}} x^i + \frac{1}{p^{j+1}} \sum_{r=0}^{e-1} \sum_{i \in C_{p^j\alpha}} x^i$$

$$= \frac{f}{p^{j+1}} \sum_{i=0}^{p^n-1} x^i + \frac{1}{p^{j+1}} \{\rho_0 \Omega_j(x) + \rho_1 \Omega_j(x^p) + \cdots + \rho_{e-1} \Omega_j(x^{p^{j-1}})\},$$

as stated in the Theorem. Further since

$$\theta_{p^j\alpha}(x) = \theta_{p^j}(x^{q-1}),$$

we get

$$\theta_{q^{p^j}}(x) = \frac{f}{p^{j+1}} \sum_{i=0}^{p^n-1} x^i + \frac{1}{p^{j+1}} \{\rho_k \Omega_j(x) + \rho_{k+1} \Omega_j(x^p) + \cdots + \rho_{k-1} \Omega_j(x^{p^{j-1}})\}.$$ 

This proves the theorem. □

**Corollary 2.** Let $p$ be an odd prime, $q$ an odd prime power such that $q$ is a primitive root mod $p^n$, $n \geq 1$ an integer. Then there are $(n + 1)$ primitive idempotents in $R_{p^n}$ given by

$$\theta_0(x) = \frac{1}{p^n} \{1 + x + x^2 + \cdots + x^{p^n-1}\},$$

$$\theta_{p^j}(x) = \frac{p-1}{p^{j+1}} \sum_{i=0}^{p^n-1} x^i - \frac{1}{p^{j+1}} \sum_{i \in C_{p^j-1}} x^i,$$

for $0 \leq j \leq n - 1$.

**Corollary 3.** If $q$ is a quadratic residue modulo $p$, then for a suitable choice of $\alpha$, all the $(2n + 1)$ primitive idempotents in $R_{p^n}$ are given by

$$\theta_0(x) = \frac{1}{p^n} \{1 + x + x^2 + \cdots + x^{p^n-1}\},$$

$$\theta_{p^j} = \frac{p-1}{2p^{j+1}} \sum_{i=0}^{p^n-1} x^i + \frac{1}{p^{j+1}} \left\{\frac{-1 + \delta}{2} \sum_{i \in C_{p^j-1}} x^i + \frac{-1 - \delta}{2} \sum_{i \in C_{q^{p^j-1}}} x^i\right\},$$
\[ \theta_{gp} = \frac{p - 1}{2p + 1} \sum_{i=0}^{p^n - 1} x^i + \frac{1}{p + 1} \left\{ \frac{-1 - \delta}{2} \sum_{i \in C_{p, j - 1}} x^i + \frac{-1 + \delta}{2} \sum_{i \in C_{gp, j - 1}} x^i \right\}, \]

for \( 0 \leq j \leq n - 1 \), where \( \delta \in \mathbb{GF}(q) \) is given by

\[ \delta^2 = \begin{cases} p & \text{if } p \equiv 1 \pmod{4}, \\ -p & \text{if } p \equiv 3 \pmod{4}. \end{cases} \]

Proof follows from Theorem 3 using Lemma 8(i) and (ii).

5. The dimension, generating polynomials and minimum distances of minimal codes of length \( p^n \)

The dimension of the minimal code \( \mathcal{M}_s \) is the number of non-zeros of the generating idempotent \( \theta_s(x) \), which is the cardinality of the cyclotomic coset \( C_s \).

**Lemma 12.** If \( \mathcal{C} \) is a cyclic code of length \( m \) generated by \( g(x) \) and is of minimum distance \( d \), then the code \( \hat{\mathcal{C}} \) of length \( mk \) generated by \( g(x)(1 + x^m + x^{2m} + \cdots + x^{(k-1)m}) \) is a repetition code of \( \mathcal{C} \) repeated \( k \) times and its minimum distance is \( dk \).

Proof is trivial.

The generating polynomial of the code \( \mathcal{M}_0 \) is clearly

\[ \frac{x^{p^n} - 1}{x - 1} = 1 + x + x^2 + \cdots + x^{p^n - 1} \]

and its minimum distance is \( p^n \).

Let \( 0 \leq j \leq n - 1 \), \( j \) fixed. We have

\[ x^{p^n - 1} = (x^{p^n - j} - 1)(1 + x^{p^n - j} + x^{2p^n - j} + \cdots + x^{(p'-1)p^n - j}), \]

where

\[ x^{p^n - j} - 1 = (x^{p^n - j - 1} - 1)(1 + x^{p^n - j - 1} + x^{2p^{n - j - 1}} + \cdots + x^{(p-1)p^{n-j-1}}). \]

One notes that

\[ \prod_{k=0}^{c-1} M^{(g^p)^{(p^k)}}(x) = (1 + x^{p^n - 1} + x^{2p^{n-j-1}} + \cdots + x^{(p-1)p^{n-j-1}}). \]

Let \( \mathcal{C}_j \) be the code of length \( p^n - j \) generated by \( g(x) = x^{p^n - j - 1} - 1 \). Then by Lemma 12, the code \( \hat{\mathcal{C}}_j \) of length \( p^n \) generated by \( (x^{p^n} - 1) / \prod_{k=0}^{c-1} M^{(g^p)^{(p^k)}}(x) \) is the repetition code of \( \mathcal{C}_j \), repeated \( p^j \) times and its minimum distance is \( 2p^j \). The minimal cyclic
Let $M$ code $a \in M$ codes $d$ further, if $f$ is odd, by Remark 1, $-1 \in \mathbb{Z}_q$, so that the minimal polynomial of $a^{\delta^j}$ is the reciprocal of the minimal polynomial of $a^{\delta^j}$. Therefore the generating polynomial of $M_{g^k, \frac{q}{p^j}}$ is negative of reciprocal of the generating polynomial of the $M_{g^k, \frac{q}{p^j}}$ and thus the minimum distance of the minimal codes $M_{g^k, \frac{q}{p^j}}$ and $M_{g^k, \frac{q}{p^j}}$ is same, for $0 \leq k \leq \frac{q}{2} - 1$ and $f$ odd.

6. Some examples of minimal ternary and 5-ary cyclic codes

**Example 1.** Let $p = 23$, $q = 3$. Since $3^{11} \equiv 1 \pmod{23}$, but $gcd(\frac{3^{11}-1}{23}, 23) = 1$, we have $e = 2$, $f = 11$. Here $g = 5$ is a primitive root mod 23. The 3-cyclotomic cosets mod 23 are

\[
C_0 = \{0\}, \quad C_1 = \{1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18\}, \quad C_5 = \{5, 7, 10, 11, 14, 15, 17, 19, 20, 21, 22\}.
\]

Further $\delta^2 \equiv -23 \pmod{3}$ gives $\delta = 1$ or $-1$, so that, by Lemma 9(ii), we can take $\eta_0 = \frac{-1+\delta}{2} = 0$, $\eta_1 = \frac{-1-\delta}{2} = -1$.

Thus the three ternary primitive idempotents mod 23 are given by

\[
\begin{align*}
\theta_0(x) &= 2(1 + x + x^2 + \cdots + x^{22}), \\
\theta_1(x) &= 1 + x^5 + x^7 + x^{10} + x^{11} + x^{14} + x^{15} + x^{17} + x^{19} + x^{20} + x^{21} + x^{22}, \\
\theta_5(x) &= 1 + x + x^2 + x^3 + x^4 + x^6 + x^8 + x^9 + x^{12} + x^{13} + x^{16} + x^{18}.
\end{align*}
\]

Further

\[
x^{23} - 1 = (x - 1)(x^{11} - x^8 - x^6 + x^4 + x^3 - x^2 - x - 1) \\
\times (x^{11} + x^{10} + x^9 - x^8 - x^7 + x^5 + x^3 - 1).
\]

If we take $M^{(1)}(x) = (x^{11} - x^8 - x^6 + x^4 + x^3 - x^2 - x - 1)$ then the minimal ternary cyclic codes $M_0$, $M_1$, $M_5$ of length 23 have the following parameters:

<table>
<thead>
<tr>
<th>Code</th>
<th>dimension</th>
<th>minimum distance</th>
<th>generating polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>$M_0$</td>
<td>1</td>
<td>23</td>
<td>$(1 + x + x^2 + \cdots + x^{22})$</td>
</tr>
<tr>
<td>$M_1$</td>
<td>11</td>
<td>9</td>
<td>$(x^{12} + x^9 + x^7 + x^6 - x^5 + x^4 - x^3 - x + 1)$</td>
</tr>
<tr>
<td>$M_5$</td>
<td>11</td>
<td>9</td>
<td>$(x^{12} - x^{11} - x^9 + x^8 - x^7 + x^6 + x^5 + x^3 + 1)$</td>
</tr>
</tbody>
</table>
Example 2. Let \( p = 13 \), \( q = 5 \). Since \( 5^4 \equiv 1 \pmod{13} \), but \( \gcd(5^4-1, 13) = 1 \), we have \( e = 3 \), \( f = 4 \). Here \( g = 2 \) is a primitive root mod 13. The 5-cyclotomic cosets mod 13 are

\[
C_0 = \{0\},
\]

\[
C_1 = \{1, 5, 8, 12\},
\]

\[
C_2 = \{2, 3, 10, 11\},
\]

\[
C_4 = \{4, 6, 7, 9\},
\]

where, by Lemma 9(iii), the characteristic equation of matrix

\[
\mathcal{A} = \begin{bmatrix}
-4 & -3 & -2 \\
1 & 2 & 1 \\
2 & 1 & 1
\end{bmatrix}
\]

is given by

\[
x^3 + x^2 + x + 1 = 0;
\]

so that eigenvalues of \( \mathcal{A} \) are 2,3,4. Also \( (2, 4, 3)^T \) is an eigenvector corresponding to the eigenvalue 2. Therefore by Corollary 1, we can take \( \eta_0 = 2 \), \( \eta_1 = 4 \), \( \eta_2 = 3 \).

Thus the four 5-ary primitive idempotents mod 13 are given by

\[
\theta_0(x) = 2(1 + x + x^2 + \cdots + x^{12}),
\]

\[
\theta_1(x) = 3 + 4(x + x^5 + x^8 + x^{12}) + 3(x^2 + x^3 + x^{10} + x^{11}) + (x^4 + x^6 + x^7 + x^9),
\]

\[
\theta_2(x) = 3 + 3(x + x^5 + x^8 + x^{12}) + (x^2 + x^3 + x^{10} + x^{11}) + 4(x^4 + x^6 + x^7 + x^9),
\]

\[
\theta_4(x) = 3 + (x + x^5 + x^8 + x^{12}) + 4(x^2 + x^3 + x^{10} + x^{11}) + 3(x^4 + x^6 + x^7 + x^9).
\]

Further

\[
x^{13} - 1 = (x - 1)(x^4 + x^3 - x^2 + x + 1)(x^4 + 2x^3 + x^2 + 2x + 1)(x^4 - 2x^3 - 2x + 1).
\]

If we take \( M^{(1)}(x) = (x^4 + x^3 - x^2 + x + 1) \), we have \( M^{(2)}(x) = (x^4 + 2x^3 + x^2 + 2x + 1) \), and \( M^{(4)}(x) = (x^4 - 2x^3 - 2x + 1) \); then the minimal 5-ary cyclic codes \( \mathcal{M}_0 \),
$\mathcal{M}_0$, $\mathcal{M}_2$, $\mathcal{M}_4$ of length 13 have the following parameters:

<table>
<thead>
<tr>
<th>Code</th>
<th>dimension</th>
<th>minimum distance</th>
<th>generating polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\mathcal{M}_0$</td>
<td>1</td>
<td>13</td>
<td>$(1 + x + x^2 + \cdots + x^{12})$</td>
</tr>
<tr>
<td>$\mathcal{M}_1$</td>
<td>4</td>
<td>8</td>
<td>$(x^9 - x^8 + 2x^7 + x^6 + x^5 - x^4 - x^3 - 2x^2 + x - 1)$</td>
</tr>
<tr>
<td>$\mathcal{M}_2$</td>
<td>4</td>
<td>8</td>
<td>$(x^9 - 2x^8 - 2x^7 - x^6 + 2x^5 - 2x^4 + x^3 + 2x^2 + 2x - 1)$</td>
</tr>
<tr>
<td>$\mathcal{M}_4$</td>
<td>4</td>
<td>8</td>
<td>$(x^9 + 2x^8 - x^7 - 2x^5 + 2x^4 + x^2 - 2x - 1)$</td>
</tr>
</tbody>
</table>

**Example 3.** Let $p = 13$, $q = 3$. Since $3^3 \equiv 1 \pmod{13}$, but $gcd(\frac{3^3 - 1}{13}, 13) = 1$, therefore we have $e = 4$, $f = 3$. Here $g = 2$ is a primitive root mod 13. The ternary cyclotomic cosets mod 13 are

\[
C_0 = \{0\}, \\
C_1 = \{1, 3, 9\}, \\
C_2 = \{2, 5, 6\}, \\
C_4 = \{4, 10, 12\}, \\
C_8 = \{7, 8, 11\},
\]

where, by Lemma 8(iv), the characteristic equation of matrix

\[
\mathcal{A} = \begin{bmatrix}
0 & 1 & 2 & 0 \\
1 & 1 & 0 & 1 \\
-3 & -2 & -3 & -2 \\
1 & 0 & 1 & 1
\end{bmatrix}
\]

is given by

\[
x^4 + x^3 - x^2 - x = 0;
\]

so that eigenvalues of $\mathcal{A}$ are 0, $-1$, $-1$. Also $(0, -1, -1)^T$ is an eigenvector belonging to the eigenvalue 0. Therefore, by Corollary 1, we can take $\eta_0 = 0$, $\eta_1 = -1$, $\eta_2 = -1$, $\eta_3 = 1$.

Thus the five ternary primitive idempotents mod 13 are given by

\[
\theta_0(x) = (1 + x + x^2 + \cdots + x^{12}), \\
\theta_1(x) = -(x^2 + x^5 + x^6) - (x^4 + x^{10} + x^{12}) + (x^8 + x^7 + x^{11}),
\]
\[ \theta_2(x) = -(x + x^3 + x^9) + (x^4 + x^{10} + x^{12}) - (x^2 + x^5 + x^6), \]
\[ \theta_4(x) = -(x + x^3 + x^9) + (x^2 + x^5 + x^6) - (x^8 + x^7 + x^{11}), \]
\[ \theta_8(x) = (x + x^3 + x^9) - (x^4 + x^{10} + x^{12}) - (x^8 + x^7 + x^{11}). \]

Further
\[ x^{13} - 1 = (x - 1)(x^3 - x - 1)(x^3 + x^2 - 1)(x^3 + x^2 + x - 1)(x^3 - x^2 - x - 1). \]

If we take \( M^{(1)}(x) = (x^3 - x - 1) \), we have \( M^{(2)}(x) = (x^3 + x^2 + x - 1) \), \( M^{(4)}(x) = (x^3 + x^2 - 1) \) and \( M^{(8)}(x) = (x^3 - x^2 - x - 1) \), then the minimal ternary cyclic codes \( \mathcal{M}_0, \mathcal{M}_1, \mathcal{M}_2, \mathcal{M}_4, \mathcal{M}_8 \) of length 13 have the following parameters:

<table>
<thead>
<tr>
<th>Code</th>
<th>dimension</th>
<th>minimum distance</th>
<th>generating polynomial</th>
</tr>
</thead>
<tbody>
<tr>
<td>( \mathcal{M}_0 )</td>
<td>1</td>
<td>13</td>
<td>((1 + x + x^2 + \cdots + x^{12}))</td>
</tr>
<tr>
<td>( \mathcal{M}_1 )</td>
<td>3</td>
<td>9</td>
<td>((x^{10} + x^8 + x^7 + x^6 - x^5 - x^4 + x^2 - x + 1))</td>
</tr>
<tr>
<td>( \mathcal{M}_2 )</td>
<td>3</td>
<td>9</td>
<td>((x^{10} - x^9 - x^7 + x^5 + x^4 + x^3 - x^2 + x + 1))</td>
</tr>
<tr>
<td>( \mathcal{M}_4 )</td>
<td>3</td>
<td>9</td>
<td>((x^{10} - x^9 + x^8 - x^6 - x^5 + x^4 + x^3 + x^2 + 1))</td>
</tr>
<tr>
<td>( \mathcal{M}_8 )</td>
<td>3</td>
<td>9</td>
<td>((x^{10} + x^9 - x^8 + x^7 + x^6 + x^5 - x^3 - x + 1))</td>
</tr>
</tbody>
</table>

References