Bull. Korean Math. Soc. **0** (0), No. 0, pp. 1–0
https://doi.org/10.4134/BKMS.b170443
pISSN: 1015-8634 / eISSN: 2234-3016

PRIMITIVE IDEMPOTENTS IN THE RING $F_4[x]/\langle x^{p^n}-1\rangle$ AND CYCLOTOMIC Q CODES

Sudhir Batra and Rekha Mathur

Abstract. The parity of cyclotomic numbers of order 2, 4 and 6 associated with 4-cyclotomic cosets modulo an odd prime p are obtained. Hence the explicit expressions of primitive idempotents of minimal cyclic codes of length p^n, $n \geq 1$ over the quaternary field F_4 are obtained. These codes are observed to be subcodes of Q codes of length p^n. Some orthogonal properties of these subcodes are discussed. The minimal cyclic codes of length 17 and 43 are also discussed and it is observed that the minimal cyclic codes of length 17 are two weight codes. Further, it is shown that a Q code of prime length is always cyclotomic like a binary duadic code and it seems that there are infinitely many prime lengths for which cyclotomic Q codes of order 6 exist.

1. Introduction

A cyclic code of length m over a finite field F_q is viewed as an ideal of the semisimple quotient ring $R_m = F_q[x]/\langle x^m - 1\rangle$, where $\gcd(m, q) = 1$. It is well known that the ring R_m can be written as the direct sum of its minimal ideals. So if we obtain the minimal ideals of R_m, then we can find all the ideals of R_m and hence all the cyclic codes of length m depending upon the different conditions imposed on m and q. Further, a minimal ideal has an idempotent generator, called primitive idempotent, therefore there is a 1-1 correspondence between the set of primitive idempotents and the set of minimal ideals of R_m. Thus it is quite significant to obtain the primitive idempotents of R_m to analyze the cyclic codes of length m. In recent years a series of papers [1–8, 10, 11, 14–16, 18, 22–24, 26, 27, 30] have been published in which primitive idempotents of R_m with different conditions imposed on m and q have been computed. A ceratin number of cases when $m = p$ and q are odd primes and the multiplicative order of q modulo p is f with $\gcd(\frac{p-1}{f}, q) = 1$ and $q^f \not\equiv 1 (\mathrm{mod}\ p^2)$ have been discussed in [25] using the theory of cyclotomic numbers. In this paper, we consider the left case, for which we obtain the parity of all

Received May 18, 2017; Accepted September 14, 2017.
2010 *Mathematics Subject Classification.* 12E20, 94B15, 11T71.
Key words and phrases. cyclic codes, duadic codes, Q codes, primitive idempotents, cyclotomic numbers.

cyclotomic numbers of order 2, 4 and 6 associated with 4-cyclotomic cosets modulo an odd prime p. It is little bit involved to obtain the parity of some of these cyclotomic numbers, particularly of cyclotomic numbers of order 6. We obtain parity of these numbers by using the classical theory of cyclotomic numbers [28] and the fact that the ring R_p is associative and commutative (see Theorems 3.15 and 3.18). Using the parity of cyclotomic numbers so obtained, we obtain the explicit expressions of primitive idempotents of R_m with $m = p^n$ and $q = 4$ such that the multiplicative order f of 4 modulo p is $\frac{p-1}{2}$, $\frac{p-1}{4}$ or $\frac{p-1}{6}$ and $4^f \not\equiv 1 (\text{mod } p^2)$ and $2^f \not\equiv 1 (\text{mod } p)$. Unlike the approach used in [25], we either need not to obtain cyclotomic numbers or have to obtain a few of them to get the expressions for primitive idempotents in R_{p^n} for various primes p (cf. see Theorems 5.3-5.6 and Examples 5.8 and 5.9). Moreover using the approach discussed in the paper we can obtain parity of cyclotomic numbers associated with arbitrary l-cyclotomic cosets modulo p, where l is any odd or even prime power with g.c.d$(l, p) = 1$. Thus we can obtain primitive idempotents in the semisimple ring $F_{2^k}[x]/\langle x^{p^n} - 1\rangle$ for any $k \geq 1$. The minimal cyclic codes generated by primitive idempotents obtained in Theorems 5.3-5.6 are subcodes of Q codes. Q codes were first defined by V. Pless [21] and have many properties analogous to binary duadic codes [12, 17]. In [12] Ding and Pless defined cyclotomic duadic codes and further proved that every binary duadic code of odd prime length is always cyclotomic. This fact enables them to obtain the number of binary duadic codes of prime length. Analogously, we also define cyclotomic Q codes of odd prime length and show that a Q code of odd prime length is always cyclotomic (see Theorem 6.5). Further, in [29] it was shown that there are infinitely many prime lengths for which binary cyclotomic codes of order $e \geq 2$ that are not quadratic residue codes, exist. Naturally, a question arises that whether there are infinitely many primes lengths for which cyclotomic Q codes of order $e \geq 2$ that are not quaternary/quadratic residue codes, exist. In Section 6 we give partial answer to this question particularly for the case $e = 6$. In this section we also discuss some orthogonal properties of the minimal cyclic codes generated by primitive idempotents in Section 5. The rest of the paper is organized as follows.

In Section 2, we obtain 4-cyclotomic cosets modulo p^n such that the multiplicative order of 4 modulo p is $f = \frac{p-1}{e}$, where $e \geq 2$ and $4^f \not\equiv 1 (\text{mod } p^2)$ and $2^f \not\equiv 1 (\text{mod } p)$ (see Theorem 2.4). In Section 3, we discuss cyclotomic numbers and some arithmetic properties of some families of R_p using the parity of cyclotomic numbers. In Section 4, we obtain certain exponential sums which are necessary to obtain the primitive idempotents. In Section 5, the explicit expressions of primitive idempotents in R_{p^n} are obtained as already mentioned and two examples are given in which the minimal cyclic codes of length 17 and 43 over F_4 are discussed. Here we observe that each minimal code of length 17 above is a two weight code with two non-zero weights 12 and 16 and may be used in defining strongly regular graph and secret sharing schemes [13].

2. Cyclotomic cosets

Throughout this paper unless otherwise stated we use the following terminology and assumptions: (i) p denotes an odd prime. (ii) F_q denotes a field of prime power order q and $F_4 = \{0, 1, \beta, \beta^2\}$, where β is a primitive element of F_4, that is, a cube root of unity. (iii) $O_m(l)$ denotes the multiplicative order of l modulo m. (iv) $R_{p^n} = F_4[x]/\langle x^{p^n} - 1\rangle$, where $n \geq 1$ and x is an indeterminate. (v) (a, b) denotes the greatest common divisor of integers $a > 0$ and $b > 0$. (vi) $O_p(4) = f = \frac{p-1}{e}$, where $e \geq 2$ is an integer and (vii) $4^f \not\equiv 1 (\text{mod } p^2)$ and $2^f \not\equiv 1 (\text{mod } p)$. Using these assumptions, we have:

Lemma 2.1. *e is an even integer.*

Proof. Let R denote the set of quadratic residues modulo p. Since R is a multiplicative group of order $\frac{p-1}{2}$ and $4 \in R$, $O_p(4)$ divides $\frac{p-1}{2}$. Hence $\frac{p-1}{f} = 2(\frac{p-1}{2})/f$, that is $p - 1 = ef$, where e is an even integer. □

Lemma 2.2. *If $O_p(4) = f$ and $4^f \not\equiv 1 \pmod{p^2}$, then $O_{p^n}(4) = fp^{n-1}$ for all $n \geq 1$.*

Proof. Follows on similar lines as in [25, Lemma 1, p. 655]. □

Lemma 2.3 ([9])**.** *There always exists a g which is a primitive root modulo p^n for each $n \geq 1$.*

Theorem 2.4. *The $en + 1$ 4-cyclotomic cosets modulo p^n are given by*

$$\Omega_0 = \{0\},$$

$$\Omega_{p^j g^k} = \{p^j g^k, 4p^j g^k, \ldots, 4^{fp^{n-j-1}-1} p^j g^k\},$$

where $0 \leq j \leq n-1$, $0 \leq k \leq e-1$ and g is a primitive root modulo p^n for each $n \geq 1$.

Proof. Follows on similar lines as in Theorem 1 of [25] using Lemma 2.2 and 2.3. □

Lemma 2.5.

(i) $2 \in \Omega_{p^0 g^{\frac{e}{2}}}$,

(ii) $-1 \in \Omega_{p^0 g^{\frac{e}{2}}}$ *when f is odd and $-1 \in \Omega_{p^0 g^0}$ when f is even.*

Proof. Since $O_p(4) = f$, $4^f \equiv 1 \pmod{p}$. Therefore, $2^{2f} \equiv 1 \pmod{p}$. Let $O_p(2) = t$. Then $2f = tk_1$ for some positive integer k_1. Also $2^{2t} \equiv 1 \pmod{p}$, i.e., $4^t \equiv 1 \pmod{p}$ which implies that $t = fk_2$ for some positive integer k_2. Thus we have $k_1 k_2 = 2$ and this is possible when $k_1 = 2$, $k_2 = 1$ or $k_1 = 1$, $k_2 = 2$. The case $k_1 = 2$, $k_2 = 1$ is not possible, because of the assumption that $2^f \not\equiv 1 \pmod{p}$. Hence $O_p(2) = 2f$. Further, by assumption $4^f \not\equiv 1 \pmod{p^2}$, $2^f \not\equiv 1 \pmod{p^2}$, therefore working on similar lines as in Lemma 2.2, we have $O_{p^n}(2) = 2fp^{n-1}$. This obviously implies $2^{fp^{n-1}} \equiv -1 \pmod{p^n}$. Now we prove (i). Since g is a primitive root modulo p^n and

$(4,p)=1$, so $4 \equiv g^b \pmod{p^n}$ for some integer b. Further by Lemma 2.2, $O_{p^n}(4) = fp^{n-1}$. Therefore, $4^{fp^{n-1}} = g^{bfp^{n-1}} \equiv 1 \pmod{p^n}$. This implies $p^{n-1}(p-1)$ divides $b\frac{(p-1)}{e}p^{n-1}$ and which in turn implies $b = et$ for some integer t. Now using $4 \equiv g^{et} \pmod{p^n}$ and the fact that e is even due to Lemma 2.1 we have $2 \equiv \pm g^{(e/2)t} \pmod{p^n}$. First let $2 \equiv g^{(e/2)t} \pmod{p^n}$. Then $-1 \equiv 2^{fp^{n-1}} \equiv g^{(e/2)tfp^{n-1}} = g^{p^{n-1}(\frac{p-1}{2})t} \equiv (-1)^t \pmod{p^n}$. Therefore, t must be odd. Second let $2 \equiv -g^{(e/2)t} \pmod{p^n}$. Then the fact $g^{p^{n-1}(\frac{p-1}{2})} \equiv -1 \pmod{p^n}$ implies that $2 \equiv g^{(e/2)(t+p^{n-1}f)} \pmod{p^n}$. Again using the fact that $2^{fp^{n-1}} \equiv -1 \pmod{p^n}$, we get that $(t+p^{n-1}f)$ is odd. Hence by Theorem 2.4, $2 \in \Omega_{p^0g^{\frac{e}{2}}}$, proving (i). In view of (i) above and Theorem 2.4, it is observed that $\Omega_{p^0g^0}$ contains all even powers of 2 and $\Omega_{p^0g^{\frac{e}{2}}}$ contains all odd powers of 2 modulo p^n. Now using the fact that $2^{fp^{n-1}} \equiv -1 \pmod{p^n}$ we have that if f is even, then $-1 \in \Omega_{p^0g^0}$ and if f is odd, then $-1 \in \Omega_{p^0g^{\frac{e}{2}}}$. □

This lemma will be used in obtaining the parity of cyclotomic numbers in Section 3 and while discussing the orthogonal properties in Section 6.

Theorem 2.6. *The $en+1$ 4-cyclotomic cosets modulo p^n obtained in Theorem 2.4 can be rewritten as*

$$\Omega_0 = \{0\},$$
$$\Omega_{p^jg^k} = \{p^jg^k(4^t+\lambda p) \,|\, 0 \le t \le f-1, 0 \le \lambda \le p^{n-j-1}-1\},$$

where $0 \le j \le n-1, 0 \le k \le e-1$ and g is a primitive root modulo p^n for each $n \ge 1$.

Proof. In view of Lemma 2.3, we can assume that g is a primitive root modulo p^n for $n = 1, 2, \ldots, n$. For $n \ge 1$, let

$$\omega_0 = \{0\},$$
$$\omega_{jk} = \{p^jg^k(4^t+\lambda p) \,|\, 0 \le t \le f-1, 0 \le \lambda \le p^{n-j-1}-1\},$$

where $0 \le j \le n-1, 0 \le k \le e-1$.

First we claim that $\cup_{k=0}^{e-1}\omega_{0k}$ is a reduced residue system modulo p^n. If not, suppose that for some $t_1 \ne t_2, \lambda_1$ and λ_2, $(4^{t_1}+\lambda_1 p) \equiv (4^{t_2}+\lambda_2 p) \pmod{p^n}$. Then $4^{t_1} \equiv 4^{t_2} \pmod{p}$, which is against our supposition that $O_p(4) = f$. If $t_1 = t_2 = t$ (say), then obviously for $\lambda_1 \ne \lambda_2$, $4^t+\lambda_1 p \not\equiv 4^t+\lambda_2 p \pmod{p^n}$. Further for any $t_1, t_2, \lambda_1, \lambda_2$ and $i \ne 0$, we must have $(4^{t_1}+\lambda_1 p) \not\equiv g^i(4^{t_2}+\lambda_2 p) \pmod{p^n}$. If not so, then $(4^{t_1}+\lambda_1 p) \equiv g^i(4^{t_2}+\lambda_2 p) \pmod{p^n}$, which implies that $4^{t_1} \equiv g^i 4^{t_2} \pmod{p}$, leading to a contradiction again. Finally, note that for each $0 \le i \le e-1$, $(g^i(4^t+\lambda p), p^n) = 1$ and $|\omega_{0i}| = p^{n-1}f$, proving the claim.

Now we claim that for any $0 \le t_1 \le f-1$, $0 \le \lambda \le p^{n-1}-1$, $1 \le i \le e-1$ and $0 \le t \le fp^{n-1}-1$, $4^{t_1}+\lambda p \not\equiv g^i 4^t \pmod{p^n}$ because otherwise $4^{t_1} \equiv g^i 4^t \pmod{p}$, leading to a contradiction as before. Summarizing all these facts we

get that $\Omega_{p^0g^0} = \omega_{00}$ and thus for any $0 \leq i \leq e-1$, $g^i\Omega_{p^0g^0} = g^i\omega_{00}$, i.e., $\Omega_{p^0g^i} = \omega_{0i}$. Working on similar lines, we can obtain that for any $1 \leq j \leq n-1$ and $0 \leq k \leq e-1$, $\Omega_{p^jg^k} = \omega_{jk}$. This proves the theorem. □

3. Cyclotomic numbers and arithmetic properties of some families in R_p

3.1. Throughout this section, we assume that $n = 1$. In view of Theorem 2.4, we have $j = 0$, and so $e+1$ 4-cyclotomic cosets modulo p are given by (i) $\Omega_0 = \{0\}$, (ii) For $0 \leq k \leq e-1$,

$$\Omega_{g^k} = \{g^k, 4g^k, \ldots, 4^{f-1}g^k\}.$$

Note that for $n = 1$, we take $\Omega_{p^0g^k} = \Omega_{g^k}$. Further using Lemma 2.5, $-1 \in \Omega_{g^0}$ when f is even and $-1 \in \Omega_{g^{\frac{e}{2}}}$ when f is odd.

Further, $R_p = F_4[x]/\langle x^p - 1\rangle$ and for $0 \leq i \leq e-1$, we assume that an element $\sum_{k\in\Omega_{g^i}} x^k \in R_p$ is denoted by X_i.

Definition 3.2 (see [12])**.** Recall that $p = ef+1$ is a prime, and g is a primitive root modulo p. Then the cyclotomic classes of order e are defined as $C_0 = (g^e)$, $C_i = g^iC_0$, $i = 1, 2, \ldots, e-1$, where (g^e) denotes the multiplicative group generated by g^e.

Lemma 3.3. *For $0 \leq k \leq e-1$, $\{\Omega_{g^k}\}$ forms the set of cyclotomic classes of order e.*

Proof. Since g be a primitive root modulo p, $g^b \equiv 4 \pmod p$ for some integer b, $1 \leq b \leq p-2$. Therefore, $O_p(4) = f$ implies that $g^{bf} \equiv 1 \pmod p$. Hence e divides b. Further, since $C_0 = (g^e)$ is a subgroup of (g) generated by g^e and e divides b, so $4 \equiv g^b \in C_0$ and therefore, $\Omega_{g^0} = \{1, 4, 4^2, \ldots, 4^{f-1}\} \subseteq C_0$. Now the multiplicative order of g^e being f, we have $C_0 = \Omega_{g^0}$. It is easy to see that $C_k = g^k\Omega_{g^0} = \Omega_{g^k}$ for each k, proving the lemma. □

Lemma 3.4 ([9])**.** $\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if} \quad p = 8k \pm 1, \\ -1 & \text{if} \quad p = 8k \pm 3. \end{cases}$

Here $(\cdot)$ denotes the Legendre symbol.

Lemma 3.5 (Euler's Criterion [9])**.** *An integer a is a quadratic residue modulo an odd prime p if and only if $a^{\frac{p-1}{2}} \equiv 1 \pmod p$.*

Theorem 3.6. *Let $O_p(4) = \frac{p-1}{e}$. Then* (i) *$p = 8k \pm 3$ for $e = 2$,* (ii) *$p = 8k+1$ for $e = 4$ and* (iii) *$p = 8k \pm 3$ for $e = 6$.*

Proof. (i) If $e = 2$, then $f = \frac{p-1}{2}$, then by our assumption $2^{\frac{p-1}{2}} \not\equiv 1 \pmod p$. Therefore, by Lemma 3.5, $\left(\frac{2}{p}\right) = -1$ and hence by Lemma 3.4, $p = 8k \pm 3$.

(ii) If $e = 4$, then $f = \frac{p-1}{4}$, which implies that $2^{\frac{p-1}{2}} \equiv 1 \pmod p$. Therefore, by Lemma 3.5, $\left(\frac{2}{p}\right) = 1$ and hence by Lemma 3.4, $p = 8k+1$. The case $p = 8k-1$ is ruled out because 4 must divide $p-1$.

(iii) If $e = 6$, then $f = \frac{p-1}{6}$, which implies that $O_p(2) = 2f = \frac{p-1}{3}$ (see proof of lemma 2.5). Now suppose that 2 is a quadratic residue modulo p. Then by Lemma 3.5, $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. On the other hand $O_p(2) = \frac{p-1}{3}$. Therefore, $\frac{p-1}{3}$ must divide $\frac{p-1}{2}$, which is not possible. Hence 2 is not a quadratic residue modulo p, and thus by Lemma 3.4, $p = 8k \pm 3$. □

Definition 3.7. (a) For fixed i and j, $0 \leq i \leq e-1$, $0 \leq j \leq e-1$, the cyclotomic numbers (i, j) of order e are defined as $(i, j) = |(C_i + 1) \cap C_j|$.

(b) The Cyclotomic matrix is the $e \times e$ matrix N whose (i, j)th entry is the cyclotomic number $(i - 1, j - 1)$.

Our next few results are related to cyclotomy and parity of cyclotomic numbers and Theorem 3.10 and Lemmas 3.11, 3.14 and 3.17 can be obtained by repeatedly using Lemmas 3 and 4 of [28] which are stated as Lemmas 3.8 and 3.9 respectively. However, the results in Theorem 3.10 and cyclotomic matrices in Lemmas 3.11 and 3.14 can be taken directly from Lemma 6 and Array I of [28] respectively.

Lemma 3.8. (a) *For any integers m and n, $(i, j) = (i + me, j + ne)$,*

(b) $(i, j) = (e - i, j - i)$,

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

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

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

Lemma 3.9. *The cyclotomic numbers $(0, h)$ are odd or even according as $2 \in C_h$ or not. In particular, exactly one of the numbers $(0, j)$ is odd.*

Theorem 3.10. (i) *Suppose $p = 8k + 3$ and $e = 2$. Then f is odd and*

$$X_i^2 = \frac{f-1}{2}X_i + \frac{f+1}{2}X_{i+1} = X_{i+1},$$
$$X_0X_1 = \frac{f-1}{2}(X_0 + X_1) + f = 1.$$

(ii) *Let $p = 8k - 3$ and $e = 2$. Then f is even and*

$$X_i^2 = \frac{f-2}{2}X_i + \frac{f}{2}X_{i+1} + f = X_{i+1},$$
$$X_0X_1 = \frac{f}{2}(X_0 + X_1) + f = X_0 + X_1,$$

where subscripts are taken to be non-neagtive integers modulo 2.

Here note that Lemma 6 of [28] provides O. Perron results (see Theorem 24, Chapter 16 in [19]) for all cases, i.e., $p = 4k \pm 1$.

Lemma 3.11. *Assume $e = 4$ and $p = 8k + 1$. Then the Cyclotomic Matrix is given by*

$$\begin{bmatrix} A & B & C & D \\ B & D & E & E \\ C & E & C & E \\ D & E & E & B \end{bmatrix}$$

where, $A + B + C + D = f - 1$, $B + D + 2E = f$ and $2(C + E) = f$. Further,

$$\begin{aligned} X_i^2 &= AX_i + BX_{i+1} + CX_{i+2} + DX_{i+3} + fx^0, \\ X_iX_{i+1} &= BX_i + DX_{i+1} + EX_{i+2} + EX_{i+3}, \\ X_iX_{i+2} &= CX_i + EX_{i+1} + CX_{i+2} + EX_{i+3}, \\ X_iX_{i+3} &= DX_i + EX_{i+1} + EX_{i+2} + BX_{i+3}, \end{aligned}$$

where subscripts are taken to be non-negative integers modulo 4.

Theorem 3.12. *The parity of cyclotomic numbers of order 4 defined in the cyclotomic matrix given in Lemma 3.11 are as follows*:

(i) *C is odd,*
(ii) *A, B, D are even,*
(iii) *E is even if k is odd and E is odd if k is even.*

Proof. By Lemma 2.5 and Notation in 3.1, $2 \in \Omega_{g^2}$. Therefore by Lemma 3.3, $2 \in C_2$ and hence by Lemma 3.9, C is odd and A, B, D are even, proving (i) and (ii). By Lemma 3.11, $C + E = k$ and by (i) C is odd and therefore (iii) follows trivially. □

Theorem 3.13. *Assume $e = 4$ and $p = 8k + 1$. Then*

(i) $X_i^2 = X_{i+2}$,

(ii) $X_iX_{i+1} = \begin{cases} 0 & \text{if } k \text{ is odd} \\ X_{i+2} + X_{i+3} & \text{if } k \text{ is even,} \end{cases}$

(iii) $X_iX_{i+2} = \begin{cases} X_i + X_{i+2} & \text{if } k \text{ is odd} \\ X_i + X_{i+1} + X_{i+2} + X_{i+3} & \text{if } k \text{ is even,} \end{cases}$

(iv) $X_iX_{i+3} = \begin{cases} 0 & \text{if } k \text{ is odd} \\ X_{i+1} + X_{i+2} & \text{if } k \text{ is even.} \end{cases}$

Proof. It follows immediately using Lemma 3.11 and Theorem 3.12. □

Lemma 3.14. *Assume $e = 6$ and $p = 8k + 3$. Then the Cyclotomic Matrix is given by*

$$\begin{bmatrix} A & B & C & D & E & F \\ G & H & I & E & C & I \\ H & J & G & F & I & B \\ A & G & H & A & G & H \\ G & F & I & B & H & J \\ H & I & E & C & I & G \end{bmatrix},$$

where $A+B+C+D+E+F = f$, $C+E+G+H+2I = f$, $B+F+G+H+I+J = f$, $2A+2G+2H = f-1$. *Further,*

$$\begin{aligned}
X_i^2 &= AX_i + BX_{i+1} + CX_{i+2} + DX_{i+3} + EX_{i+4} + FX_{i+5},\\
X_iX_{i+1} &= GX_i + HX_{i+1} + IX_{i+2} + EX_{i+3} + CX_{i+4} + IX_{i+5},\\
X_iX_{i+2} &= HX_i + JX_{i+1} + GX_{i+2} + FX_{i+3} + IX_{i+4} + BX_{i+5},\\
X_iX_{i+3} &= AX_i + GX_{i+1} + HX_{i+2} + AX_{i+3} + GX_{i+4} + HX_{i+5} + fx^0,\\
X_iX_{i+4} &= GX_i + FX_{i+1} + IX_{i+2} + BX_{i+3} + HX_{i+4} + JX_{i+5},\\
X_iX_{i+5} &= HX_i + IX_{i+1} + EX_{i+2} + CX_{i+3} + IX_{i+4} + GX_{i+5},
\end{aligned}$$

where subscripts are taken to be non-negative integers modulo 6.

Theorem 3.15. *The parity of cyclotomic numbers of order 6 defined in Lemma 3.14 are as follows*:

(i) D *is odd,* A, B, C, E, F *are even,*

(ii) G *and* H *are of opposite parity,*

(iii) I, J *are always odd.*

Proof. (i) By Lemma 2.5 and Lemma 3.4, $2 \in \Omega_{g^3} = C_3$ and therefore (i) follows due to Lemma 3.9.

(ii) Using $C+E+G+H+2I = f$ due to Lemma 3.14 and (i) above we get that $G+H$ is odd.

(iii) (a) Let G be odd and H be even. We now evaluate $X_0X_1X_3$ in R_p by repeatedly using the expressions for X_iX_j given in Lemma 3.14, $X_0X_3 = X_1 + X_4 + 1$ and $(X_0X_3)X_1 = X_1^2 + X_4X_1 + X_1 = X_4 + X_1 + X_2 + X_5 + 1$. $X_0X_1 = X_0 + IX_2 + IX_5$. Let I be even, then $X_0X_1 = X_0$. This implies that, $(X_0X_1)X_3 = X_4 + X_1 + 1$. Therefore $(X_0X_3)X_1 \neq (X_0X_1)X_3$, which is a contradiction because R_p is associative and commutative and thus I must be odd.

Now let J be even. Then using the fact that I is odd as above and evaluating $X_0X_2^2$ in R_p, we have $X_0X_2 = X_2 + X_4$. Therefore, $(X_0X_2)X_2 = (X_2 + X_4)X_2 = X_5 + X_4 + X_0$, while $(X_0X_2)X_2 = X_0X_2^2 = X_0X_5 = X_1 + X_4 + X_5$, this leads to a contradiction, thus J must be odd.

(b) Let G be even and H be odd. We now evaluate $X_0X_1X_3$ in R_p. For, $X_0X_3 = X_2 + X_5 + 1$ and $(X_0X_3)X_1 = X_1 + X_1X_2 + X_1X_5 = X_1 + X_2 + IX_3 + IX_0 + IX_3 + X_5 + JX_0$. Let I and J be even, then $(X_0X_3)X_1 = X_1 + X_2 + X_5$, $X_0X_1 = X_1$. This implies that, $(X_0X_1)X_3 = X_1$. Therefore $(X_0X_3)X_1 \neq (X_0X_1)X_3$, which is a contradiction because R_p is associative and commutative.

Let J be even and I be odd. Then, evaluating $X_0X_2^2$ yet again, $(X_0X_2)X_2 = (X_0 + X_4)X_2 = X_0X_2 + X_2X_4 = X_0 + X_4 + X_2 + X_0 = X_2 + X_4$. While $X_0X_2^2 = X_0X_5 = X_0 + X_1 + X_4$, which leads to a contradiction again.

Finally, let J be odd and I be even. Then, $(X_0X_2)X_2 = (X_0 + X_1)X_2 = X_0 + X_1 + X_2$ and $X_0X_2^2 = X_0X_5 = X_0$, which leads to a contradiction again. Hence I and J both are odd. □

Theorem 3.16. *Assume $e = 6$ and $p = 8k + 3$. Then*

(i) $X_i^2 = X_{i+3}$,

(ii) $X_iX_{i+1} = \begin{cases} X_i + X_{i+2} + X_{i+5} & \text{if } G \text{ is odd} \\ X_{i+1} + X_{i+2} + X_{i+5} & \text{if } G \text{ is even,} \end{cases}$

(iii) $X_iX_{i+2} = \begin{cases} X_{i+1} + X_{i+2} + X_{i+4} & \text{if } G \text{ is odd} \\ X_i + X_{i+1} + X_{i+4} & \text{if } G \text{ is even,} \end{cases}$

(iv) $X_iX_{i+3} = \begin{cases} 1 + X_{i+1} + X_{i+4} & \text{if } G \text{ is odd} \\ 1 + X_{i+2} + X_{i+5} & \text{if } G \text{ is even,} \end{cases}$

(v) $X_iX_{i+4} = \begin{cases} X_i + X_{i+2} + X_{i+5} & \text{if } G \text{ is odd} \\ X_{i+2} + X_{i+4} + X_{i+5} & \text{if } G \text{ is even,} \end{cases}$

(vi) $X_iX_{i+5} = \begin{cases} X_{i+1} + X_{i+4} + X_{i+5} & \text{if } G \text{ is odd} \\ X_i + X_{i+1} + X_{i+4} & \text{if } G \text{ s even.} \end{cases}$

Proof. It follows immediately using Lemma 3.14 and Theorem 3.15. □

Lemma 3.17. *Assume $e = 6$ and $p = 8k - 3$. Then the Cyclotomic Matrix is given by*

$$\begin{bmatrix} A & B & C & D & E & F \\ B & F & G & H & I & G \\ C & G & E & I & J & H \\ D & H & I & D & H & I \\ E & I & J & H & C & G \\ F & G & H & I & G & B \end{bmatrix},$$

where $A + B + C + D + E + F = f - 1$, $B + F + 2G + H + I = f$, $C + G + E + I + J + H = f$, $2D + 2H + 2I = f$. Further,

$$\begin{aligned} X_i^2 &= AX_i + BX_{i+1} + CX_{i+2} + DX_{i+3} + EX_{i+4} + FX_{i+5} + fx^0, \\ X_iX_{i+1} &= BX_i + FX_{i+1} + GX_{i+2} + HX_{i+3} + IX_{i+4} + GX_{i+5}, \\ X_iX_{i+2} &= CX_i + GX_{i+1} + EX_{i+2} + IX_{i+3} + JX_{i+4} + HX_{i+5}, \\ X_iX_{i+3} &= DX_i + HX_{i+1} + IX_{i+2} + DX_{i+3} + HX_{i+4} + IX_{i+5}, \\ X_iX_{i+4} &= EX_i + IX_{i+1} + JX_{i+2} + HX_{i+3} + CX_{i+4} + GX_{i+5}, \\ X_iX_{i+5} &= FX_i + GX_{i+1} + HX_{i+2} + IX_{i+3} + GX_{i+4} + BX_{i+5}, \end{aligned}$$

where subscripts are taken to be non-negative integers modulo 6.

Theorem 3.18. *The parity of cyclotomic numbers of order 6 defined in Lemma 3.17 are as follows*:

(i) *D is odd, A, B, C, E, F are even,*

(ii) *H and I are of same parity,*

(iii) *G and J are of same parity,*

(iv) *G and H are of same parity and so are I and J.*

Proof. (i) By Lemma 2.5 and Lemma 3.3, $2 \in \Omega_{g^3} = C_3$ and therefore (i) follows due to Lemma 3.9.

(ii) Using $B + F + 2G + H + I = f$ given in Lemma 3.17 and (i) above we get that $H + I$ is even.

(iii) Using the equation $C + E + G + J + H + I = f$ given in Lemma 3.17 and (i) and (ii) above we get that $G + J$ is even.

(iv) On contrary suppose that G and H are of opposite parity. We now evaluate $X_0^2X_1$ in R_p by repeatedly using the expressions for X_iX_j given in Lemma 3.17.

(a) Let G be odd and H be even. Then $X_0^2 = X_3$ and so $X_0^2X_1 = X_3X_1 = X_2 + X_5$. Also $X_0^2X_1 = X_0(X_0X_1) = X_0(X_2 + X_5) = X_1 + X_4 + X_1 + X_4 = 0$, which is a contradiction, proving (iv) in this case.

(b) Let G be even and H be odd. Then $X_0^2 = X_3$ and so $X_0^2X_1 = X_3X_1 = X_0 + X_4$. Also $X_0^2X_1 = X_0(X_0X_1) = X_0(X_3 + X_4) = X_0 + X_1 + X_2 + X_3 + X_4 + X_5 + X_1 + X_3 = X_0 + X_2 + X_4 + X_5$, which is a contradiction, proving (iv) in this case also. □

Theorem 3.19. *Assume $e = 6$ and $p = 8k - 3$. Then*

(i) $X_i^2 = X_{i+3}$,

(ii) $X_iX_{i+1} = \begin{cases} X_{i+2} + X_{i+3} + X_{i+4} + X_{i+5} & \text{if } G \text{ is odd} \\ 0 & \text{if } G \text{ is even,} \end{cases}$

(iii) $X_iX_{i+2} = \begin{cases} X_{i+1} + X_{i+3} + X_{i+4} + X_{i+5} & \text{if } G \text{ is odd} \\ 0 & \text{if } G \text{ is even,} \end{cases}$

(iv) $X_iX_{i+3} = \begin{cases} X_i + X_{i+1} + X_{i+2} + X_{i+3} + X_{i+4} + X_{i+5} & \text{if } G \text{ is odd} \\ X_i + X_{i+3} & \text{if } G \text{ is even,} \end{cases}$

(v) $X_iX_{i+4} = \begin{cases} X_{i+1} + X_{i+2} + X_{i+3} + X_{i+5} & \text{if } G \text{ is odd} \\ 0 & \text{if } G \text{ is even,} \end{cases}$

(vi) $X_iX_{i+5} = \begin{cases} X_{i+1} + X_{i+2} + X_{i+3} + X_{i+4} & \text{if } G \text{ is odd} \\ 0 & \text{if } G \text{ is even.} \end{cases}$

Proof. It follows immediately using Lemma 3.17 and Theorem 3.18. □

4. Exponential sums

4.1. Recall that $R_{p^n} = F_4[x]/\langle x^{p^n} - 1\rangle$. Suppose that for $0 \le j \le n - 1$, $0 \le k \le e - 1$, an element $X_{jk}(x)$ of R_{p^n} is given by $X_{jk}(x) = \sum_{l \in \Omega_{p^j g^k}} x^l$.

For $n = 1$, set $X_{0k}(x) = X_k(x)$ where $0 \le k \le e - 1$.

Let α denote a primitive p^nth root of unity and δ denote a primitive pth root of unity in some extension field of F_4.

Further, we write $X_{ij}(x) = X_{ij}$, $X_i(x) = X_i$ and $Y_i = X_i(\delta)$.

Theorem 4.2. *Assume $e = 2$. Then δ can be suitably chosen such that* (i) *$Y_0 = \beta$, $Y_1 = \beta^2$, when $p = 8k + 3$ and* (ii) *$Y_0 = \beta$, $Y_1 = \beta^2$, when $p = 8k - 3$.*

Proof. (i) By Theorem 3.10(i), for $0 \le i \le 1$, $Y_i^2 = Y_{i+1}$ and $Y_0Y_1 = 1$. Therefore, we can choose δ such that $Y_0 = \beta$ and $Y_1 = \beta^2$.

(ii) By Theorem 3.10(ii), for $0 \le i \le 1$, $Y_i^2 = Y_{i+1}$ and $Y_0Y_1 = Y_0 + Y_1$. Therefore, we can choose δ such that $Y_0 = \beta$ and $Y_1 = \beta^2$. □

Theorem 4.3. *Assume $e = 4$ and $p = 8k + 1$. Then δ can be suitably chosen such that* (i) $Y_0 = \beta$, $Y_1 = 0$, $Y_2 = \beta^2$, $Y_3 = 0$, *when k is odd and* (ii) $Y_0 = 1$, $Y_1 = \beta$, $Y_2 = 1$, $Y_3 = \beta^2$, *when k is even.*

Proof. (i) By Theorem 3.13, $Y_0^2 = Y_2$, $Y_0Y_2 = Y_0 + Y_2$, so that $Y_0^3 = Y_0 + Y_0^2$. This implies $Y_0(1 + Y_0 + Y_0^2) = 0$. Then $Y_0 = 0$ or $1 + Y_0 + Y_0^2 = 0$. Taking $1 + Y_0 + Y_0^2 = 0$ we have $Y_0 = \beta$ and $Y_2 = Y_0^2 = \beta^2$ (Here $Y_0 = 0$ can also be considered, for explanation see Remark 4.6). Again by Theorem 3.13, $Y_1Y_2 = 0$. Since $Y_2 = \beta^2 \neq 0$, so we have $Y_1 = 0$ and $Y_3 = Y_1^2 = 0$.

(ii) By Theorem 3.13, $Y_i^2 = Y_{i+2}$, $Y_0Y_1 = Y_2 + Y_3$, $Y_0Y_3 = Y_1 + Y_2$. Adding last two equations we get $Y_0Y_1 + Y_0Y_3 = Y_1 + Y_3$, which implies that $(Y_0 - 1)(Y_1 + Y_3) = 0$. Then $Y_0 = 1$ or $Y_1 = Y_3$. Taking $Y_0 = 1$ we get $Y_2 = Y_0^2 = 1$. Now again by Theorem 3.13, $Y_0Y_2 = Y_0 + Y_1 + Y_2 + Y_3 = 1$, we get that $Y_1 + Y_1^2 + 1 = 0$ and which implies $Y_1 = \beta$ or β^2. Now δ can be suitably chosen so that $Y_1 = \beta$. Then $Y_3 = Y_1^2 = \beta^2$, proving the result. □

Theorem 4.4. *Assume $p = 8k + 3$ and $e = 6$. Then* (i) $Y_0 = 0 = Y_3$, $Y_1 = 1 = Y_4$, $Y_2 = \beta$, $Y_5 = \beta^2$, *when G is even and* (ii) $Y_0 = 1 = Y_3$, $Y_1 = 0 = Y_4$, $Y_2 = \beta$, $Y_5 = \beta^2$, *when G is odd.*

Proof. (i) By Theorem 3.16, $Y_i^2 = Y_{i+3}$. Putting this in the identity $1 + Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 = 0$, we get

$$Y_0 + Y_0^2 + Y_1 + Y_1^2 + Y_2 + Y_2^2 = 1. \tag{1}$$

Again by Theorem 3.16, $Y_i^3 = Y_iY_{i+3} = 1 + Y_{i+2} + Y_{i+5} = 1 + Y_{i+2} + Y_{i+2}^2$. In view of this equation, (1) reduces to $Y_0^3 + Y_1^3 + Y_2^3 = 0$. The possible solutions of this equation are (a) $Y_0 = Y_1 = Y_2 = 0$, (b) $Y_0^3 = 0$, $Y_1^3 = Y_2^3 = 1$, (c) $Y_1^3 = 0$, $Y_0^3 = Y_2^3 = 1$ and (d) $Y_2^3 = 0$, $Y_0^3 = Y_1^3 = 1$.

The set of values in (a) leads to a contradiction due to identity (3). So (a) is ruled out.

Due to symmetry among three other solutions we choose solution (b) for definiteness (see Remark 4.6 for more explanation). We can suitably choose δ such that (b) holds and then by Theorem 3.16, $0 = Y_0^3 = Y_0Y_3 = 1 + Y_2 + Y_5$. This implies that $Y_2 = \beta$ and $Y_5 = \beta^2$. Again using Theorem 3.16, $1 = Y_2^3 = Y_2Y_5 = 1 + Y_1 + Y_4$ implying that $Y_1 = Y_4 = 1$. The case $Y_1 = Y_4 = 0$ is not possible, because $Y_1^3 = 1$. Finally, $Y_0^3 = 0$ implies that $Y_0 = 0$ and $Y_3 = Y_0^2 = 0$.

(ii) Working on similar lines as in (i) above, we get that

$$Y_0 + Y_0^2 + Y_1 + Y_1^2 + Y_2 + Y_2^2 = 1. \tag{2}$$

Now by Theorem 3.16, $Y_3^2 = Y_0$ and $Y_iY_{i+3} = Y_i^3 = 1 + Y_{i+1} + Y_{i+1}^2$. In view of above equation (2) reduces to $Y_1^3 + Y_2^3 + Y_3^3 = 0$. Now as discussed in (i) and by repeated applications of Theorem 3.16, we get (ii). □

Theorem 4.5. *Assume $p = 8k-3$ and $e = 6$. Then* (i) $Y_0 = \beta$, $Y_3 = \beta^2$, $Y_1 = 1 = Y_4$, $Y_2 = 1 = Y_5$, *when G is odd and* (ii) $Y_0 = \beta$, $Y_3 = \beta^2$, $Y_1 = 0 = Y_4$, $Y_2 = 0 = Y_5$, *when G is even.*

Proof. (i) By Theorem 3.19, $Y_i^2 = Y_{i+3}$ and $Y_iY_{i+3} = Y_i + Y_{i+1} + Y_{i+2} + Y_{i+3} + Y_{i+4} + Y_{i+5}$. Now using $Y_0Y_3 = Y_0^3 = Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5$ and the fact that $1 + Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 = 0$, we get $Y_0^3 = 1$. Similarly, $Y_1^3 = Y_2^3 = Y_3^3 = Y_4^3 = Y_5^3 = 1$. Since, $Y_i^2 = Y_{i+3}$, so we can take $Y_0 = \beta$, $Y_3 = \beta^2$, $Y_1 = \beta$, $Y_4 = \beta^2$, $Y_2 = \beta$ and $Y_5 = \beta^2$. This leads to a contradiction because $Y_iY_{i+1} = Y_{i+2} + Y_{i+3} + Y_{i+4} + Y_{i+5}$. Similarly, another set of values $Y_0 = 1 = Y_3$, $Y_1 = \beta$, $Y_4 = \beta^2$, $Y_2 = \beta$, $Y_5 = \beta^2$, also leads to a contradiction. Thus we must have the solution as described in (i) (for explanation see Remark 4.6 also).

(ii) By Theorem 3.19, $Y_i^2 = Y_{i+3}$ which implies $Y_i^3 = Y_iY_{i+3} = Y_i + Y_{i+3}$. Now using the identity $1 + Y_0 + Y_1 + Y_2 + Y_3 + Y_4 + Y_5 = 0$, we have $1 + Y_0^3 + Y_1^3 + Y_2^3 = 0$. One of the solution of this equation is $Y_0^3 = Y_1^3 = Y_2^3 = 1$. Again by Theorem 3.19, $Y_iY_j = 0$ when $j \neq i, i+3$. So $Y_0^3 = Y_1^3 = Y_2^3 = 1$ is not possible. Therefore, we may choose δ such that $Y_0^3 = 1$ and $Y_1^3 = 0 = Y_2^3$. Now $Y_0Y_3 = Y_0 + Y_3$ implies that $Y_0 = \beta$, $Y_3 = \beta^2$. Trivially, $Y_1 = 0 = Y_4$ and $Y_2 = 0 = Y_5$. □

Remark 4.6. While proving Theorem 4.3(i) if we take $Y_0 = 0$, then $Y_2 = Y_0^2 = 0$. Therefore, $1 + Y_0 + Y_1 + Y_2 + Y_3 = 0$ implies that $Y_1 = \beta$ and $Y_3 = \beta^2$. If we consider this solution, then this will permute the idempotents corresponding to various cyclotomic cosets obtained in Theorem 5.4. Similarly in Theorem 4.3(ii), if instead of taking $Y_0 = 1$ we take $Y_1 = Y_3$. Then $Y_1 = Y_3 = 1$, $Y_0 = \beta$ and $Y_2 = \beta^2$. While proving Theorem 4.4(i) if we consider solution by taking case (c) or (d), then again this will permute the idempotents corresponding to various cyclotomic cosets obtained in Theorem 5.5. Similarly, in Theorem 4.5(i) we can also take $Y_0 = Y_3 = Y_2 = Y_5 = 1$, $Y_1 = \beta$ and $Y_4 = \beta^2$ or $Y_0 = Y_3 = Y_1 = Y_4 = 1$, $Y_2 = \beta$ and $Y_5 = \beta^2$ etc. as the solution.

Lemma 4.7. *Let $i \in \Omega_{p^lg^m}$, where $0 \leq l \leq n-1$ and $0 \leq m \leq e-1$. Then for any $0 \leq j \leq n-1$, $0 \leq k \leq e-1$ and f even* $\sum_{r\in\Omega_{p^jg^k}} \alpha^{-ir} =$

$$\begin{cases} 0 & \text{if} \quad j+l < n-1 \\ p^{n-j-1}X_{n-1,k+m}(\alpha) & \text{if} \quad j+l = n-1 \\ |\Omega_{p^jg^k}| & \text{if} \quad j+l \geq n. \end{cases}$$

Proof. If $i \in \Omega_{p^lg^m}$, then by Theorem 2.6, $i = p^lg^m(4^{t_1} + \lambda_1 p)$ for some $0 \leq t_1 \leq f-1$ and $0 \leq \lambda_1 \leq p^{n-l-1} - 1$. Therefore, $\sum_{r\in\Omega_{p^jg^k}} \alpha^{-ir} = \sum_r \alpha^{-p^lg^m(4^{t_1}+\lambda_1 p)r}$. Now f being even, so by Lemma 2.5, $-1 \in \Omega_{p^0g^0}$ and therefore,

$$\sum_{r\in\Omega_{p^jg^k}} \alpha^{-ir} = \sum_r \alpha^{p^lg^m(4^{t_1}+\lambda_1 p)r}$$

$$= \sum_{t=0}^{f-1} \sum_{\lambda=0}^{p^{n-j-1}-1} \alpha^{p^l g^m (4^{t_1}+\lambda_1 p)} \alpha^{p^j g^k (4^t+\lambda p)}$$

$$= \sum_{t=0}^{f-1} \sum_{\lambda=0}^{p^{n-j-1}-1} \alpha^{p^{l+j} g^{k+m} (4^{t_1}+\lambda_1 p)(4^t+\lambda p)}. \tag{3}$$

(i) Let $l+j < n-1$. Then $\alpha^{p^{l+j} g^{k+m}(4^{t_1}+\lambda_1 p)} = \gamma$ is a primitive $p^{n-(l+j)}$th root of unity. Then (3) becomes

$$\begin{aligned}
\sum_{r \in \Omega_{p^j g^k}} \alpha^{-ir} &= \sum_t \sum_\lambda \gamma^{(4^t+\lambda p)} \\
&= \sum_t \gamma^{4^t} \sum_\lambda \gamma^{\lambda p} \\
&= \sum_t \gamma^{4^t} (1 + \gamma^p + \cdots + \gamma^{(p^{n-j-1}-1)p}) \\
&= \frac{(\gamma^p)^{p^{n-j-1}} - 1}{\gamma^p - 1} \sum_t \gamma^{4^t}.
\end{aligned}$$

Since $j + l < n-1$ and γ is a primitive $p^{n-(l+j)}$ th root of unity, $\gamma^p \neq 1$ and $(\gamma^p)^{p^{n-j-1}} = 1$. Therefore, $\sum_t \sum_\lambda \gamma^{(4^t+\lambda p)} = 0$, proving (i).

(ii) Let $j + l = n-1$. Then $\alpha^{p^{(l+j)}(4^{t_1}+\lambda_1 p)} = \gamma$ is a primitive pth root of unity. Substituting this in (3) we get

$$\begin{aligned}
\sum_{r \in \Omega_{p^j g^k}} \alpha^{-ir} &= \sum_t \sum_\lambda \gamma^{g^{k+m}(4^t+\lambda p)} \\
&= \sum_t \gamma^{g^{k+m} 4^t} \sum_\lambda (\gamma^p)^{\lambda g^{k+m}} \\
&= \sum_t \gamma^{g^{k+m} 4^t} (p^{n-j-1}) \\
&= p^{n-j-1} X_{n-1,k+m}(\alpha).
\end{aligned}$$

(iii) $j + l \geq n$. Again let $\gamma = \alpha^{p^{l+j} g^{k+m}(4^{t_1}+\lambda_1 p)}$. Then $\gamma = 1$ and therefore, $\sum_{r \in \Omega_{p^j g^k}} \alpha^{-ir} = |\Omega_{p^j g^k}|$. □

Lemma 4.8. *Let $i \in \Omega_{p^l g^m}$, where $0 \leq l \leq n-1$ and $0 \leq m \leq e-1$. Then for any $0 \leq j \leq n-1$, $0 \leq k \leq e-1$ and f odd we have* $\sum_{r \in \Omega_{p^j g^k}} \alpha^{-ir} =$

$$\begin{cases} 0 & \text{if} \quad j + l < n-1 \\ p^{n-j-1} X_{n-1,k+m+e/2}(\alpha) & \text{if} \quad j + l = n-1 \\ |\Omega_{p^j g^{(k+e/2)}}| & \text{if} \quad j + l \geq n. \end{cases}$$

Proof. Since f is odd, by Lemma 2.5, $-1 \in \Omega_{p^0 g^{\frac{e}{2}}}$, therefore, $\sum_{r \in \Omega_{p^j g^k}} \alpha^{-ir} = \sum_{r \in \Omega_{p^j g^{(k+\frac{e}{2})}}} \alpha^{ir}$. The proof now follows on similar lines as in Lemma 4.7. □

5. Expressions of idempotents

In this section we provide explicit expressions for primitive idempotents in R_{p^n} over F_4 in all the cases, i.e., when $e = 2, 4$ or 6 corresponding to 4-cyclotomic cosets $\Omega_{p^j q^k}$ obtained in Theorem 2.4. For this we recall some definitions and some well known facts without proof.

It is well known that a q-cyclotomic coset Ω_s modulo n corresponds to a minimal polynomial, say, $M_s(x)$. Then, the cyclic code of length n, say, E_s over F_q is the minimal cyclic code with generator polynomial $g_s(x) = \frac{x^n-1}{M_s(x)}$ and the number of these minimal cyclic codes is equal to the number of q-cyclotomic cosets modulo n. Further, observe that every minimal cyclic code with generator polynomial $g_s(x)$ such that $M_s(x) \neq (x-1)$ is even like and the code with generator polynomial $g_0(x) = \frac{x^n-1}{(x-1)}$ is odd like.

Lemma 5.1 ([19,25]). *If α is a primitive (p^n) th root of unity in some extension field of F_q, then the primitive idempotent corresponding to a $q-$cyclotomic coset Ω_s is given by $\theta_s(x) = \sum_{i=0}^{p^n-1} \epsilon_i^{(s)} x^i$, where $\epsilon_i^s = \frac{1}{p^n} \sum_{j\in\Omega_s} \alpha^{-ij}$.*

Also note that $\theta_s(\alpha^i) = \begin{cases} 1, & i \in \Omega_s \\ 0 & \text{otherwise.} \end{cases}$

Therefore, the defining set of the code generated by θ_s is $\{0, 1, 2, \ldots, p^n - 1\} - \Omega_s$ and due to the above discussion, $E_s = \langle \theta_s(x) \rangle = \langle g_s(x) \rangle$. Hence the number of primitive idempotents θ_s are equal to the number of cyclotomic cosets Ω_s.

For $0 \leq j \leq n-1$ and $0 \leq k \leq e-1$, let θ_{jk} denote the primitive idempotent corresponding to $\Omega_{p^j g^k}$ and θ_0 denote the primitive idempotent corresponding to Ω_0. Further, let E_t denote the minimal cyclic code generated by the primitive idempotent θ_t and $\bar{E}_t$ denote the cyclic code generated by the idempotent $1+\theta_t$.

Theorem 5.2. (i) *If f is even, then for $0 \leq j \leq n-1$ and $0 \leq k \leq e-1$ the $en+1$ primitive idempotents in R_{p^n} are given by $\theta_0 = 1 + x + x^2 + \cdots + x^{p^n-1}$ and $\theta_{jk} = \sum_{i=0}^{e-1} X_{(n-j-1)i} Y_{(i+k)}$.*

(ii) *If f is odd, then for $0 \leq j \leq n-1$ and $0 \leq k \leq e-1$ the $en+1$ primitive idempotents in R_{p^n} are given by $\theta_0 = 1 + x + x^2 + \cdots + x^{p^n-1}$ and $\theta_{jk} = 1 + \sum_{l=0}^{e-1} \sum_{k=1}^{j} X_{(n-k)l} + \sum_{i=0}^{e-1} X_{(n-j-1)i} Y_{(i+k+e/2)}$.*

Proof. It can be easily proved that θ_0 in (i) and (ii) above is a primitive idempotent corresponding to Ω_0.

(i) By Lemma 5.1 and Theorem 2.4,

$$\theta_{jk} = \epsilon_0^{p^j g^k} + \epsilon_{p^0 g^0}^{p^j g^k} \sum_{i\in\Omega_{p^0 g^0}} x^i + \cdots + \epsilon_{p^0 g^{e-1}}^{p^j g^k} \sum_{i\in\Omega_{p^0 g^{e-1}}} x^i + \epsilon_{p^1 g^0}^{p^j g^k} \sum_{i\in\Omega_{p^1 g^0}} x^i$$
$$+ \cdots + \epsilon_{p^1 g^{e-1}}^{p^j g^k} \sum_{i\in\Omega_{p^1 g^{e-1}}} x^i + \cdots + \epsilon_{p^{n-1} g^0}^{p^j g^k} \sum_{i\in\Omega_{p^{n-1} g^0}} x^i$$

$$+\cdots+\epsilon_{p^{n-1}g^{e-1}}^{p^jg^k}\sum_{i\in\Omega_{p^{n-1}g^{e-1}}}x^i. \tag{4}$$

We now evaluate $\epsilon_r^{p^jg^k}$, where $r \in \{0, p^0g^0, \ldots, p^0g^{e-1}, \ldots, p^{n-1}g^0, \ldots, p^{n-1}g^{e-1}\}$ by using definition of ϵ_i^s given in Lemma 5.1.

For $\epsilon_0^{p^jg^k} = \frac{1}{p^n}\sum_{t\in\Omega_{p^jg^k}}\alpha^{-0t} = |\Omega_{p^jg^k}|$ and by Lemma 4.7,

$$\epsilon_{p^lg^m}^{p^jg^k} = \begin{cases} 0 & \text{if} \quad j+l < n-1 \\ p^{n-j-1}X_{n-1,k+m}(\alpha) & \text{if} \quad j+l = n-1 \\ |\Omega_{p^jg^k}| & \text{if} \quad j+l \geq n. \end{cases}$$

Since f is even, $|\Omega_{p^jg^k}| = p^{n-j-1}f = 0$. Further, in view of Theorem 2.6, $X_{(n-1)(k+m)}(\alpha) = X_{0(k+m)}(\delta) = Y_{k+m}$. Using these facts and various ϵ_i^s's, (4) reduces to $\theta_{jk} = \sum_{i=0}^{e-1} X_{(n-j-1)i}Y_{(i+k)}$.

Similarly, we can obtain (ii). □

In Theorems 5.3-5.6 we give the explicit expressions for primitive idempotents in all the specific cases when $e = 2, 4$ or 6. These expressions can be easily obtained from the general expressions given in Theorem 5.2 by using Theorems 4.2-4.5. Since the odd like primitive idempotent θ_0, an all one vector of length p^n remains same in all cases, therefore only expressions of even like primitive idempotents θ_{jk} will be listed.

Theorem 5.3. *Assume $e = 2$ and $0 \leq j \leq n-1$. Then*

(i) *If $p = 8k+3$, then the expressions of $2n$ primitive idempotents are given by*

$$\begin{aligned}\theta_{j0} &= 1 + X_{(n-j)0} + X_{(n-j)1} + \cdots + X_{(n-1)0} + X_{(n-1)1} \\ &\quad + \beta^2 X_{(n-j-1)0} + \beta X_{(n-j-1)1}, \\ \theta_{j1} &= 1 + X_{(n-j)0} + X_{(n-j)1} + \cdots + X_{(n-1)0} + X_{(n-1)1} \\ &\quad + \beta X_{(n-j-1)0} + \beta^2 X_{(n-j-1)1}.\end{aligned}$$

(ii) *If $p = 8k-3$, then the expressions for primitive idempotents are given by*

$$\begin{aligned}\theta_{j0} &= \beta X_{(n-j-1)0} + \beta^2 X_{(n-j-1)1}, \\ \theta_{j1} &= \beta^2 X_{(n-j-1)0} + \beta X_{(n-j-1)1}.\end{aligned}$$

Remark. The expressions for idempotents in the above theorem have also been obtained in [2, 6]. In particular for $n = 1$, E_{00} and E_{01} are expurgated QR codes and $\bar{E}_{00}$ and $\bar{E}_{01}$ are augmented QR codes over F_4 (see [19] for detail).

Theorem 5.4. *Assume $p = 8k+1$, $e = 4$ and $0 \leq j \leq n-1$. Then*

(i) *If k is odd, then the expressions of $4n$ primitive idempotents are given by*

$$\begin{aligned}\theta_{j0} &= \beta X_{(n-j-1)0} + \beta^2 X_{(n-j-1)2}, \\ \theta_{j1} &= \beta^2 X_{(n-j-1)1} + \beta X_{(n-j-1)3},\end{aligned}$$

$$\theta_{j2} = \beta^2 X_{(n-j-1)0} + \beta X_{(n-j-1)2},$$
$$\theta_{j3} = \beta X_{(n-j-1)1} + \beta^2 X_{(n-j-1)3}.$$

(ii) *If k is even, then the expressions of $4n$ primitive idempotents are given by*

$$\theta_{j0} = X_{(n-j-1)0} + \beta X_{(n-j-1)1} + X_{(n-j-1)2} + \beta^2 X_{(n-j-1)3},$$
$$\theta_{j1} = \beta X_{(n-j-1)0} + X_{(n-j-1)1} + \beta^2 X_{(n-j-1)2} + X_{(n-j-1)3},$$
$$\theta_{j2} = X_{(n-j-1)0} + \beta^2 X_{(n-j-1)1} + X_{(n-j-1)2} + \beta X_{(n-j-1)3},$$
$$\theta_{j3} = \beta^2 X_{(n-j-1)0} + X_{(n-j-1)1} + \beta X_{(n-j-1)2} + X_{(n-j-1)3}.$$

Theorem 5.5. *Assume $p = 8k+3$, $e = 6$ and $0 \leq j \leq n-1$. Then*

(i) *If G is even, then the expressions of $6n$ primitive idempotents are given by*

$$\begin{aligned}
\theta_{j0} &= 1 + X_{(n-j)0} + X_{(n-j)1} + \cdots + X_{(n-j)5} + X_{(n-j+1)0} + \cdots + X_{(n-1)5} \\
&\quad + X_{(n-j-1)1} + \beta^2 X_{(n-j-1)2} + X_{(n-j-1)4} + \beta X_{(n-j-1)5}, \\
\theta_{j1} &= 1 + X_{(n-j)0} + X_{(n-j)1} + \cdots + X_{(n-j)5} + X_{(n-j+1)0} + \cdots + X_{(n-1)5} \\
&\quad + X_{(n-j-1)0} + \beta^2 X_{(n-j-1)1} + X_{(n-j-1)3} + \beta X_{(n-j-1)4}, \\
\theta_{j2} &= 1 + X_{(n-j)0} + X_{(n-j)1} + \cdots + X_{(n-j)5} + X_{(n-j+1)0} + \cdots + X_{(n-1)5} \\
&\quad + \beta^2 X_{(n-j-1)0} + X_{(n-j-1)2} + \beta X_{(n-j-1)3} + X_{(n-j-1)5}, \\
\theta_{j3} &= 1 + X_{(n-j)0} + X_{(n-j)1} + \cdots + X_{(n-j)5} + X_{(n-j+1)0} + \cdots + X_{(n-1)5} \\
&\quad + X_{(n-j-1)1} + \beta X_{(n-j-1)2} + X_{(n-j-1)4} + \beta^2 X_{(n-j-1)5}, \\
\theta_{j4} &= 1 + X_{(n-j)0} + X_{(n-j)1} + \cdots + X_{(n-j)5} + X_{(n-j+1)0} + \cdots + X_{(n-1)5} \\
&\quad + X_{(n-j-1)0} + \beta X_{(n-j-1)1} + X_{(n-j-1)3} + \beta^2 X_{(n-j-1)4}, \\
\theta_{j5} &= 1 + X_{(n-j)0} + X_{(n-j)1} + \cdots + X_{(n-j)5} + X_{(n-j+1)0} + \cdots + X_{(n-1)5} + \\
&\quad \beta X_{(n-j-1)0} + X_{(n-j-1)2} + \beta^2 X_{(n-j-1)3} + X_{(n-j-1)5}.
\end{aligned}$$

(ii) *If G is odd, then the expressions of $6n$ primitive idempotents are given by*

$$\begin{aligned}
\theta_{j0} &= 1 + X_{(n-j)0} + X_{(n-j)1} + \cdots + X_{(n-j)5} + X_{(n-j+1)0} + \cdots + X_{(n-1)5} \\
&\quad + X_{(n-j-1)0} + \beta^2 X_{(n-j-1)2} + X_{(n-j-1)3} + \beta X_{(n-j-1)5}, \\
\theta_{j1} &= 1 + X_{(n-j)0} + X_{(n-j)1} + \cdots + X_{(n-j)5} + X_{(n-j+1)0} + \cdots + X_{(n-1)5} \\
&\quad + \beta^2 X_{(n-j-1)1} + X_{(n-j-1)2} + \beta X_{(n-j-1)4} + X_{(n-j-1)5}, \\
\theta_{j2} &= 1 + X_{(n-j)0} + X_{(n-j)1} + \cdots + X_{(n-j)5} + X_{(n-j+1)0} + \cdots + X_{(n-1)5} \\
&\quad + \beta^2 X_{(n-j-1)0} + X_{(n-j-1)1} + \beta X_{(n-j-1)3} + X_{(n-j-1)4}, \\
\theta_{j3} &= 1 + X_{(n-j)0} + X_{(n-j)1} + \cdots + X_{(n-j)5} + X_{(n-j+1)0} + \cdots + X_{(n-1)5} \\
&\quad + X_{(n-j-1)0} + \beta X_{(n-j-1)2} + X_{(n-j-1)3} + \beta^2 X_{(n-j-1)5},
\end{aligned}$$

$$\theta_{j4} = 1 + X_{(n-j)0} + X_{(n-j)1} + \cdots + X_{(n-j)5} + X_{(n-j+1)0} + \cdots + X_{(n-1)5} + \beta X_{(n-j-1)1} + X_{(n-j-1)2} + \beta^2 X_{(n-j-1)4} + X_{(n-j-1)5},$$
$$\theta_{j5} = 1 + X_{(n-j)0} + X_{(n-j)1} + \cdots + X_{(n-j)5} + X_{(n-j+1)0} + \cdots + X_{(n-1)5} + \beta X_{(n-j-1)0} + X_{(n-j-1)1} + \beta^2 X_{(n-j-1)3} + X_{(n-j-1)4}.$$

Theorem 5.6. *Assume $p = 8k - 3$, $e = 6$ and $0 \leq j \leq n - 1$. Then*

(i) *If G is odd, then the expressions of $6n$ primitive idempotents are given by*

$$\theta_{j0} = \beta X_{(n-j-1)0} + X_{(n-j-1)1} + X_{(n-j-1)2} + \beta^2 X_{(n-j-1)3} + X_{(n-j-1)4} + X_{(n-j-1)5},$$
$$\theta_{j1} = X_{(n-j-1)0} + X_{(n-j-1)1} + \beta^2 X_{(n-j-1)2} + X_{(n-j-1)3} + X_{(n-j-1)4} + \beta X_{(n-j-1)5},$$
$$\theta_{j2} = X_{(n-j-1)0} + \beta^2 X_{(n-j-1)1} + X_{(n-j-1)2} + X_{(n-j-1)3} + \beta X_{(n-j-1)4} + X_{(n-j-1)5},$$
$$\theta_{j3} = \beta^2 X_{(n-j-1)0} + X_{(n-j-1)1} + X_{(n-j-1)2} + \beta X_{(n-j-1)3} + X_{(n-j-1)4} + X_{(n-j-1)5},$$
$$\theta_{j4} = X_{(n-j-1)0} + X_{(n-j-1)1} + \beta X_{(n-j-1)2} + X_{(n-j-1)3} + X_{(n-j-1)4} + \beta^2 X_{(n-j-1)5},$$
$$\theta_{j5} = X_{(n-j-1)0} + \beta X_{(n-j-1)1} + X_{(n-j-1)2} + X_{(n-j-1)3} + \beta^2 X_{(n-j-1)4} + X_{(n-j-1)5}.$$

(ii) *If G is even, then the expressions of $6n$ primitive idempotents are given by*

$$\theta_{j0} = \beta X_{(n-j-1)0} + \beta^2 X_{(n-j-1)3},$$
$$\theta_{j1} = \beta^2 X_{(n-j-1)2} + \beta X_{(n-j-1)5},$$
$$\theta_{j2} = \beta^2 X_{(n-j-1)1} + \beta X_{(n-j-1)4},$$
$$\theta_{j3} = \beta^2 X_{(n-j-1)0} + \beta X_{(n-j-1)3},$$
$$\theta_{j4} = \beta X_{(n-j-1)2} + \beta^2 X_{(n-j-1)5},$$
$$\theta_{j5} = \beta X_{(n-j-1)1} + \beta^2 X_{(n-j-1)4}.$$

Next we present two examples illustrating the results obtained in previous sections. First we state a result related to the minimum distance of a cyclic code.

Theorem 5.7 ([20, p. 115])**.** *If $\mathcal{C}$ is a cyclic code of length m over F_q whose generator polynomial $g(x)$ has roots β, β^2, ..., $\beta^{\delta-1}$ in some extension field of F_q, then the minimum distance of $\mathcal{C}$ is $\geq \delta$, where β is a primitive mth root of unity.*

Example 5.8. Let $p = 17$. Observe that $f = \frac{17-1}{4} = 4$ and $e = 4$. $g = 7$ is a primitive root modulo 17. Then using Theorem 2.4 and Notation in 3.1, the 4-cyclotomic cosets modulo 17 are $\Omega_0 = \{0\}$, $\Omega_{7^0} = \{1, 4, 16, 13\}$, $\Omega_{7^1} = \{10, 6, 7, 11\}$, $\Omega_{7^2} = \{9, 2, 8, 15\}$ and $\Omega_{7^3} = \{3, 12, 14, 5\}$. Since $p = 8k+1 = 17$, so $k = 2$ and therefore, by Theorem 5.4(ii), the five primitive idempotents of $E_0, E_{00}, E_{01}, E_{02}$ and E_{03} are given by

$$\begin{aligned}
\theta_0(x) &= 1 + x + x^2 + \cdots + x^{16},\\
\theta_{00}(x) &= (x + x^4 + x^{16} + x^{13}) + \beta(x^6 + x^7 + x^{10} + x^{11}),\\
&\quad + (x^2 + x^8 + x^9 + x^{15}) + \beta^2(x^3 + x^5 + x^{12} + x^{14}),\\
\theta_{01}(x) &= \beta(x + x^4 + x^{16} + x^{13}) + (x^6 + x^7 + x^{10} + x^{11})\\
&\quad + \beta^2(x^2 + x^8 + x^9 + x^{15}) + (x^3 + x^5 + x^{12} + x^{14}),\\
\theta_{02}(x) &= (x + x^4 + x^{16} + x^{13}) + \beta^2(x^6 + x^7 + x^{10} + x^{11})\\
&\quad + (x^2 + x^8 + x^9 + x^{15}) + \beta(x^3 + x^5 + x^{12} + x^{14}),\\
\theta_{03}(x) &= \beta^2(x + x^4 + x^{16} + x^{13}) + (x^6 + x^7 + x^{10} + x^{11})\\
&\quad + (x^2 + x^8 + x^9 + x^{15}) + \beta(x^3 + x^5 + x^{12} + x^{14}).
\end{aligned}$$

Let for $0 \le i \le 3$, $M_{0i}(x)$ denote the minimal polynomial corresponding to the cyclotomic coset Ω_{7^i} and $M_0(x)$ denote the minimal polynomial corresponding to the cyclotomic coset Ω_0. We obtain these polynomials by repeated applications of Theorem 4.3(ii) and are given by

$$\begin{aligned}
M_0(x) &= x - 1,\\
M_{00}(x) &= x^4 + x^3 + x^4 + \beta x^2 + x + 1,\\
M_{01}(x) &= x^4 + \beta x^3 + x^2 + \beta x + 1,\\
M_{02}(x) &= x^4 + x^3 + \beta^2 x^2 + x + 1,\\
M_{03}(x) &= x^4 + \beta^2 x^3 + x^2 + \beta^2 x + 1.
\end{aligned}$$

Therefore the generator polynomials $g_0(x)$ and $g_{0i}(x)$ of E_0 and E_{0i}, where $0 \le i \le 3$, are respectively given as follows:

$$\begin{aligned}
g_0(x) &= 1 + x + x^2 + \cdots + x^{16},\\
g_{00}(x) &= x^{13} + x^{12} + \beta^2 x^{11} + x^9 + \beta^2 x^8 + \beta x^7 + \beta x^6 + \beta^2 x^5\\
&\quad + x^4 + \beta^2 x^2 + x + 1,\\
g_{01}(x) &= x^{13} + \beta x^{12} + \beta x^{11} + \beta^2 x^{10} + x^9 + \beta x^7 + \beta x^6 + x^4\\
&\quad + \beta^2 x^3 + \beta x^2 + \beta x + 1,\\
g_{02}(x) &= x^{13} + x^{12} + \beta x^{11} + x^9 + \beta x^8 + \beta^2 x^7 + \beta^2 x^6 + \beta x^5 + x^4\\
&\quad + \beta x^2 + x + 1,\\
g_{03}(x) &= x^{13} + \beta^2 x^{12} + \beta^2 x^{11} + \beta x^{10} + x^9 + \beta^2 x^7 + \beta^2 x^6 + x^4
\end{aligned}$$

$$+\beta x^3+\beta^2x^2+\beta^2x+1.$$

Using $g_{00}(x)$ we did an exhaustive search for finding the weights of all codewords in E_{00} and we find that E_{00} is a two weight code with two non-zero weights 12 and 16. The weight distribution of this code is given by $1+204z^{12}+51z^{16}$. Further, since E_{00}, E_{01}, E_{02} and E_{03} are equivalent codes, so each of these codes has the weight distribution as above.

Example 5.9. Let $p=43$. Observe that $f=\frac{43-1}{6}=7$ and $e=6$. $g=5$ is a primitive root modulo 43. Then the 4-cyclotomic cosets modulo 43 are

$$\begin{aligned}
\Omega_{5^0}&=\{1,4,16,21,41,35,11\},\\
\Omega_{5^1}&=\{5,20,37,19,33,3,12\},\\
\Omega_{5^2}&=\{25,14,13,9,36,15,17\},\\
\Omega_{5^3}&=\{39,27,22,2,8,32,42\},\\
\Omega_{5^4}&=\{23,6,24,10,40,31,38\},\\
\Omega_{5^5}&=\{29,30,34,7,28,26,18\}.
\end{aligned}$$

Since $p=8k+3$, in order to apply Theorem 5.5, we have to obtain the parity of the cyclotomic number G defined in the cyclotomic matrix given in Lemma 3.14. For this observe that $1+\Omega_g=\{6,21,38,20,34,4,13\}$ contains exactly 2 elements of Ω_{g^0}. Therefore, $G=2$, which is even. Thus by Theorem 5.5(i), the primitive idempotents of E_0, E_{00}, E_{01}, E_{02}, E_{03}, E_{04} and E_{05} are given by

$$\begin{aligned}
\theta_0&=1+x+x^2+\cdots+x^{42},\\
\theta_{00}&=1+X_1+\beta^2X_2+X_4+\beta X_5,\\
\theta_{01}&=1+X_0+\beta^2X_1+X_3+\beta X_4,\\
\theta_{02}&=1+\beta^2X_0+X_2+\beta X_3+X_5,\\
\theta_{03}&=1+X_1+\beta X_2+X_4+\beta^2X_5,\\
\theta_{04}&=1+X_0+\beta X_1+X_3+\beta^2X_4,\\
\theta_{05}&=1+\beta X_0+X_2+\beta^2X_3+X_5.
\end{aligned}$$

Let for $0\le i\le 5$, $M_{0i}(x)$ denote the minimal polynomial corresponding to the cyclotomic coset Ω_{5^i} and $M_0(x)$ denote the minimal polynomial corresponding to the cyclotomic coset Ω_0. By repeated applications of Theorem 4.4(i), we obtain these polynomials and are given by

$$\begin{aligned}
M_0(x)&=x-1,\\
M_{00}(x)&=x^7+\beta^2x^5+x^4+x^3+\beta x^2+1,\\
M_{01}(x)&=x^7+x^6+\beta^2x^5+\beta x^2+x+1,\\
M_{02}(x)&=x^7+\beta x^6+\beta x^5+\beta x^4+\beta^2x^3+\beta^2x^2+\beta^2x+1,\\
M_{03}(x)&=x^7+\beta x^5+x^4+x^3+\beta^2x^2+1,
\end{aligned}$$

$$M_{04}(x) = x^7 + x^6 + \beta x^5 + \beta^2 x^2 + x + 1,$$
$$M_{05}(x) = x^7 + \beta^2 x^6 + \beta^2 x^5 + \beta^2 x^4 + \beta x^3 + \beta x^2 + \beta x + 1.$$

Therefore the generator polynomials $g_0(x)$ and $g_{0i}(x)$ of E_0 and E_{0i}, where $0 \leq i \leq 5$, are respectively given as follows:

$$\begin{aligned}
g_0(x) &= 1 + x + x^2 + \cdots + x^{42},\\
g_{00}(x) &= x^{36} + \beta^2 x^{34} + x^{33} + \beta^2 x^{32} + \beta x^{31} + \beta^2 x^{29} + \beta^2 x^{28} + \beta x^{27}\\
&\quad + \beta^2 x^{26} + \beta x^{25} + x^{23} + x^{22} + \beta^2 x^{21} + \beta x^{20} + x^{19} + x^{17}\\
&\quad + \beta x^{16} + \beta x^{15} + x^{14} + x^{13} + \beta^2 x^{11} + \beta x^{10} + \beta^2 x^9 + \beta x^8\\
&\quad + \beta x^7 + \beta^2 x^5 + \beta x^4 + x^3 + \beta x^2 + 1,\\
g_{01}(x) &= x^{36} + x^{35} + \beta x^{34} + x^{33} + x^{31} + \beta x^{30} + \beta x^{29} + \beta x^{28} + \beta x^{26}\\
&\quad + x^{24} + \beta x^{23} + x^{22} + x^{21} + \beta^2 x^{19} + x^{18} + \beta x^{17} + x^{15} + x^{14}\\
&\quad + \beta^2 x^{13} + x^{12} + \beta^2 x^{10} + \beta^2 x^8 + \beta^2 x^7 + \beta^2 x^6 + x^5 + x^3\\
&\quad + \beta^2 x^2 + x + 1,\\
g_{02}(x) &= x^{36} + \beta x^{35} + x^{34} + \beta^2 x^{33} + \beta^2 x^{32} + x^{30} + \beta x^{29} + x^{26} + \beta^2 x^{25}\\
&\quad + x^{24} + x^{23} + x^{21} + \beta x^{20} + \beta x^{19} + x^{18} + \beta^2 x^{17} + \beta^2 x^{16} + x^{15}\\
&\quad + x^{13} + x^{12} + \beta x^{11} + x^{10} + \beta^2 x^7 + x^6 + \beta x^4 + \beta x^3 + x^2 + \beta^2 x + 1,\\
g_{03}(x) &= x^{36} + \beta x^{34} + x^{33} + \beta x^{32} + \beta^2 x^{31} + \beta x^{29} + \beta x^{28} + \beta^2 x^{27} + \beta x^{26}\\
&\quad + \beta^2 x^{25} + x^{23} + x^{22} + \beta x^{21} + \beta^2 x^{20} + x^{19} + x^{17} + \beta^2 x^{16} + \beta^2 x^{15}\\
&\quad + x^{14} + x^{13} + \beta x^{11} + \beta^2 x^{10} + \beta x^9 + \beta^2 x^8 + \beta^2 x^7 + \beta x^5 + \beta^2 x^4\\
&\quad + x^3 + \beta^2 x^2 + 1,\\
g_{04}(x) &= x^{36} + x^{35} + \beta^2 x^{34} + x^{33} + x^{31} + \beta^2 x^{30} + \beta^2 x^{29} + \beta^2 x^{28} + \beta^2 x^{26}\\
&\quad + x^{24} + \beta^2 x^{23} + x^{22} + x^{21} + \beta x^{19} + x^{18} + \beta^2 x^{17} + x^{15} + x^{14}\\
&\quad + \beta x^{13} + x^{12} + \beta x^{10} + \beta x^8 + \beta x^7 + \beta x^6 + x^5 + x^3 + \beta x^2 + x + 1,\\
g_{05}(x) &= x^{36} + \beta^2 x^{35} + x^{34} + \beta x^{33} + \beta x^{32} + x^{30} + \beta^2 x^{29} + x^{26} + \beta x^{25}\\
&\quad + x^{24} + x^{23} + x^{21} + \beta^2 x^{20} + \beta^2 x^{19} + x^{18} + \beta x^{17} + \beta x^{16}\\
&\quad + x^{15} + x^{13} + x^{12} + \beta^2 x^{11} + x^{10} + \beta x^7 + x^6 + \beta^2 x^4 + \beta^2 x^3\\
&\quad + x^2 + \beta x + 1.
\end{aligned}$$

It can be readily observed that $\alpha^{22}, \alpha^{23}, \ldots, \alpha^{34}$ are among the roots of generator polynomial of E_{00}. Therefore, using Theorem 5.7, its minimum distance $d \geq 14$. Further, one can observe that the largest set of consecutive powers of α which are among the roots of a generator polynomial of any minimal cyclic code $E_{00}, E_{01}, E_{02}, E_{03}$ or E_{04} contains not more than 13 elements and these codes

are equivalent codes. Therefore, the lower bound for the minimum distance of each code E_{0i}, where $0 \leq i \leq 5$ is 14.

6. Orthogonal properties of codes E_{jm} and cyclotomic Q codes

6.1. (i) Q Codes (see [21] for detail). Let p be an odd prime. Then a pair of sets D_0 and D_1 each of which is a union of non-zero 4-cyclotomic cosets, forms a splitting of p^n determined by μ if $\mu D_0 = D_1$, $\mu D_1 = D_0$, $D_0 \cap D_1 = \phi$ and $D_0 \cup D_1 = \{1, 2, \ldots, p^n - 1\}$, where μ is an invertible element of $\{0, 1, 2, \ldots, p-1\}$. Then a pair of cyclic codes of length p^n, $\mathcal{C}_1 = \langle e_1 \rangle$ and $\mathcal{C}_2 = \langle e_2 \rangle$ generated by idempotents e_1 and e_2, is said to be a pair of Q codes if $e_1 = a + \beta \sum_{i \in D_0} x^i + \beta^2 \sum_{i \in D_1} x^i$ and $e_2 = a + \beta^2 \sum_{i \in D_0} x^i + \beta \sum_{i \in D_1} x^i$, where a is 0 or 1.

(ii) If $n = 1$ and D_0 and D_1 in (i) are the sets of quadratic residues and non residues modulo p respectively, then $\mathcal{C}_1$ and $\mathcal{C}_2$ above are called *quaternary QR codes* (see [21]).

Using the definition of binary cyclotomic duadic codes [12] we can naturally define cyclotomic Q codes as follows.

(iii) Cyclotomic Q Codes. Let $n = 1$. If each set of the pair D_0, D_1 in (i) is a union of cyclotomic classes of order e (cf. Definition 3.2). Then the pair Q codes of length p, $\mathcal{C}_1 = \langle e_1 \rangle$ and $\mathcal{C}_2 = \langle e_2 \rangle$ defined in (i) is said to be a pair of cyclotomic Q codes of order e.

Before proving some results related to cyclotomic Q codes we first analyze some orthogonal properties of the codes E_{0i} of length p, where $0 \leq i \leq e-1$ in our next Theorem 6.4. For this we recall the following definitions of inner products and a result in [21].

Definition 6.2. Let V be a vector space of all n-tuples over F_4 and C be a code of length n over F_4. For $a \in F_4$, we take $\tilde{a} = a^2$. Let $x = \{a_0, a_1, \ldots, a_{n-1}\}$, $y = \{b_0, b_1, \ldots, b_{n-1}\} \in V$. We now define two inner products denoted by $\cdot$ and $\star$ as follows: $x \cdot y = \sum_{i=0}^{n-1} a_i \tilde{b_i}$ and $x \star y = \sum_{i=0}^{n-1} a_i b_i$. We say that x is orthogonal to y if $x \cdot y = 0$ and x is strictly orthogonal to y if $x \star y = 0$. Further we denote $C^{\perp}(C^{\perp\star})$ the orthogonal of C with respect to $\cdot(\star)$.

Theorem 6.3 ([20, 21]). *If $\mathcal{C}$ is a cyclic code of length n over F_4 with idempotent generator e, then $C^{\perp}$ has idempotent generator $1 + \mu_{-2}(e)$ and $C^{\perp\star}$ has idempotent generator $1 + \mu_{-1}(e)$, where μ_a is the coordinate permutation defined as $\mu_a : i \to ai \pmod n$ for $i \in \{0, 1, \ldots, (n-1)\}$, where a is an integer such that $(a, n) = 1$.*

Recall that for $0 \leq j \leq n-1$ and $0 \leq k \leq e-1$, let E_{jk} denote the code generated by θ_{jk} and $\bar{E}_{jk}$ denote the code generated by $1 + \theta_{jk}$.

Theorem 6.4. *Let $0 \leq k \leq \frac{e}{2} - 1$ be fixed ($e = 2, 4$ or 6). Then for any $0 \leq j \leq n-1$, E_{jk} and $E_{j(k+e/2)}$ are subcodes of some Q codes satisfying*

(I) *If $p = 8k + 3$, then $E_{jk}^{\perp} = \bar{E}_{jk}$, $E_{j(k+e/2)}^{\perp} = \bar{E}_{j(k+e/2)}$, $E_{jk}^{\perp\star} = \bar{E}_{j(k+e/2)}$ and $E_{0(i+e/2)}^{\perp\star} = \bar{E}_{0i}$*

(II) *If* $p = 8k-3$ *or* $8k+1$, *then* $E_{jk}^{\perp} = \bar{E}_{j(k+e/2)}$, $E_{j(k+e/2)}^{\perp} = \bar{E}_{jk}$, $E_{jk}^{\perp\star} = \bar{E}_{jk}$ *and* $E_{j(k+e/2)}^{\perp\star} = \bar{E}_{j(k+e/2)}$

Proof. First we prove that for $0 \le k \le \frac{e}{2} - 1$ and $0 \le j \le n-1$, E_{jk} and $E_{j(k+e/2)}$ are subcodes of some Q codes. For this, let $e = 2$. Then $p = 8k \pm 3$. Let $S_1 = \cup_{j=0}^{n-1} \Omega_{p^j g^0}$ and $S_2 = \cup_{j=0}^{n-1} \Omega_{p^j g^1}$. Here we see that $S_1 \cup S_2 = \{1, 2, \ldots, p^n - 1\}$ and $S_1 \cap S_2 = \phi$. Further, $gS_1 = S_2$ and $gS_2 = S_1$. Therefore, (S_1, S_2) is a splitting modulo p^n. Now in view of Theorem 5.3(i),

$$\sum_{j=0}^{n-1} \theta_{j0} = n + \sum_{j=1}^{n-1} (n-j)(X_{(n-j)0} + X_{(n-j)1}) + \beta^2 \sum_{j=1}^{n} X_{(n-j)0} + \beta \sum_{j=1}^{n} X_{(n-j)1}$$

and

$$\sum_{j=0}^{n-1} \theta_{j1} = n + \sum_{j=1}^{n-1} (n-j)(X_{(n-j)0} + X_{(n-j)1}) + \beta \sum_{j=1}^{n} X_{(n-j)0} + \beta^2 \sum_{j=1}^{n} X_{(n-j)1}$$

and in view of Theorem 5.3(ii) we have,

$$\sum_{j=0}^{n-1} \theta_{j0} = \beta \sum_{j=1}^{n} X_{(n-j)0} + \beta^2 \sum_{j=1}^{n} X_{(n-j)1}$$

and

$$\sum_{j=0}^{n-1} \theta_{j1} = \beta^2 \sum_{j=1}^{n} X_{(n-j)0} + \beta \sum_{j=1}^{n} X_{(n-j)1}.$$

Now observe that in both the cases, $\mu_g(\theta_{j0}) = \theta_{j1}$ and $\mu_g(\theta_{j1}) = \theta_{j0}$. Hence $\langle \sum_{j=0}^{n-1} \theta_{j0} \rangle$ and $\langle \sum_{j=0}^{n-1} \theta_{j1} \rangle$ are Q codes. Similarly, in view of Theorems 5.4-5.6, we get that $\langle \sum_{j=0}^{n-1} \theta_{j0} \rangle$ and $\langle \sum_{j=0}^{n-1} \theta_{j1} \rangle$ are Q codes in various cases and hence the result follows.

We now prove (I). For this, let $p = 8k+3$ then f is odd and therefore by Lemma 2.5, $-1 \in \Omega_{p^0 g^{e/2}}$ and $-2 \in \Omega_{p^0 g^0}$. Therefore, using the formulation of cyclotomic cosets in Theorem 2.4, $-\Omega_{p^j g^k} = \Omega_{p^j g^{k+e/2}}$ and $-2\Omega_{p^j g^k} = \Omega_{p^j g^k}$, for any $0 \le k \le \frac{e}{2} - 1$ and $0 \le j \le n-1$. This implies that $\mu_{-1}(X_{jk}) = X_{j(k+e/2)}$ and $\mu_{-1}(X_{jk}) = X_{j(k+e/2)}$ $\mu_{-2}(X_{jk}) = X_{jk}$. Hence the result follows in view of Definition 6.2 and the expressions of idempotents in Theorems 5.3(i) and 5.5. To prove (II), let $p = 8k-3$ or $8k+1$ then f is even and therefore by Lemma 2.5, $-2 \in \Omega_{p^0 g^{e/2}}$ and $-1 \in \Omega_{p^0 g^0}$. Hence the result follows on similar

lines as in (I), in view of Definition 6.2 and the expressions of idempotents in Theorems 5.3(ii), 5.4 and 5.6. □

Analogous to the fact that every binary duadic code of prime length is a cyclotomic duadic code, we see in view of Definitions 6.1(i), (ii) and Lemma 3.3 that:

Theorem 6.5. *Every Q code of prime length is cyclotomic.*

Further, the following results related to cyclotomic Q codes of order 4 and 6 are analogous to Theorems 30 and 36 of [12].

Recall that $X_i = \sum_{i \in C_i} x^i$.

Theorem 6.6. *Assume that $p = 8k + 1$ such that 4 is a biquadratic residue modulo p and 2 is not a biquadratic residue modulo p. Then there are cyclotomic Q codes of order 4 other than binary QR codes.*

Proof. Since 4 is a biquadratic residue modulo p. Then there exists an integer a such that $a^4 \equiv 4 \pmod{p}$. Let g be a primitive root modulo p. Then $a = g^b$ for some integer b and so $g^{4b} \equiv 4 \pmod{p}$. This implies $1 \equiv g^{b(p-1)} \equiv 4^{\frac{p-1}{4}} \pmod{p}$. Now $O_p(4) = f$, so we have $\frac{p-1}{4} = ft$ for some integer t. Let $D_0 = (g^{4t})$. Then D_0 is a subgroup of $C_0 = (g^4)$ with $|D_0| = f$. It is easy to see that $C_0 = D_0 \cup g^4 D_0 \cup \cdots \cup g^{4(t-1)} D_0$. Since $g^{4b} \equiv 4 \pmod{p}$, $g^{4bf} \equiv 4^f \equiv 1 \pmod{p}$ and therefore, $p - 1$ divides $4bf$, that is, t divides b. Thus $4 = g^{4b} \in (g^{4t})$. Now $|D_0| = f$. Therefore, the cyclotomic coset $\{1, 4, 4^2, \ldots, 4^{f-1}\} = D_0 \subseteq C_0$. Hence each cyclotomic class of order 4 is a union of 4-cyclotomic cosets modulo p. Now using Definition 3.2 of cyclotomic classes of order 4, we have 3 splittings, namely, $(C_0 \cup C_1, C_2 \cup C_3)$, $(C_0 \cup C_3, C_1 \cup C_2)$ and $(C_0 \cup C_2, C_1 \cup C_3)$. The first 2 splittings are determined by g^2 while the third one is determined by g. We now claim that $(X_0 + X_2)$, $(X_1 + X_3)$; $\beta(X_0 + X_1) + \beta^2(X_2 + X_3)$, $\beta^2(X_0+X_1)+\beta(X_2+X_3)$; $\beta(X_0+X_3)+\beta^2(X_1+X_2)$, $\beta^2(X_0+X_3)+\beta(X_1+X_2)$ are idempotents. Since 2 is a quadratic residue of a prime of the form $8k+1$, so we can take $b^2 \equiv 2 \pmod{p}$. Now let $b = g^l$. Then $g^{2l} \equiv 2 \pmod{p}$. Since 2 is not a biquadratic residue modulo p, l must be odd. Therefore $2 \in C_2$, proving the claim. Further, observe that $(C_0 \cup C_2)$, $(C_1 \cup C_3)$ are the sets of quadratic residues and non residues modulo p respectively. This shows that $(X_0 + X_2)$ and $(X_1 + X_3)$ are binary QR codes of length p (see [21] for detail) and the remaining two splittings give two pairs of Q codes of order 4. □

Theorem 6.7. *Assume that $p = 6f + 1$ such that 4 is a sextic residue modulo p and 2 ia quadratic non residue modulo p. Then there are cyclotomic Q codes of order 6 that are not quaternary QR codes.*

Proof. Since 2 is a quadratic non residue modulo p, $p = 8k \pm 3$. Since 4 is a sextic residue modulo p. Then there exists an integer a such that $a^6 \equiv 4 \pmod{p}$. Now working on similar lines as in Theorem 6.6, we can prove that each cyclotomic class of order 6 is a union of 4-cyclotomic cosets modulo p.

Using the definition of cyclotomic classes of order 6, we have the splittings $(C_0 \cup C_1 \cup C_2, C_3 \cup C_4 \cup C_5)$, $(C_3 \cup C_1 \cup C_2, C_0 \cup C_4 \cup C_5)$, $(C_0 \cup C_1 \cup C_5, C_3 \cup C_4 \cup C_2)$ and $(C_0 \cup C_2 \cup C_4, C_1 \cup C_3 \cup C_5)$. All these four splittings of p are determined by g^3. Further, it is easy to see that $2 \in C_3$, which in fact implies that $\beta(X_0 + X_1 + X_2) + \beta^2(X_3 + X_4 + X_5)$, $\beta^2(X_0 + X_1 + X_2) + \beta(X_3 + X_4 + X_5)$; $\beta(X_3 + X_1 + X_2) + \beta^2(X_0 + X_4 + X_5)$, $\beta^2(X_3 + X_1 + X_2) + \beta(X_0 + X_4 + X_5)$; $\beta(X_0 + X_1 + X_5) + \beta^2(X_3 + X_4 + X_2)$, $\beta^2(X_0 + X_1 + X_5) + \beta(X_3 + X_4 + X_2)$; $\beta(X_0 + X_2 + X_4) + \beta^2(X_1 + X_3 + X_5)$, $\beta^2(X_0 + X_2 + X_4) + \beta(X_1 + X_3 + X_5)$ are idempotents. Finally, we can see that the first three splittings give three pairs of cyclotomic Q codes of order 6 and the last splitting give a pair of quaternary QR codes (see [21, p. 266] for detail). □

At the end of this section, we discuss about the infinite number of prime lengths for which cyclotomic Q codes of order 6 exist. For this we need some intermediate results.

Lemma 6.8. *An integer a is a cubic residue modulo m if and only if $-a$ is a cubic residue modulo m.*

Proof. Trivial. □

Lemma 6.9 ([12])**.** *Let $p \equiv 1 \pmod 3$ be a prime. Then 2 is a cubic residue modulo p if and only if p is of the form $p = x^2 + 27y^2$, where $x, y \in Z$.*

Lemma 6.10 ([12])**.** *An integer a is a sextic residue modulo a prime p if and only if it is both a quadratic and cubic residue modulo p.*

Lemma 6.11. *Let $p \equiv 1 \pmod 3$ be a prime. Then 4 is a cubic residue modulo p if and only if 2 is a cubic residue modulo p.*

Proof. Let 2 be a cubic residue modulo p. Then there exists an integer x such that $x^3 \equiv 2 \pmod p$, $(x^2)^3 \equiv 4 \pmod p$. Therefore, 4 is a cubic residue modulo p. Now let 4 be a cubic residue modulo p. Obviously, 4 is a quadratic residue modulo p, therefore by Lemma 6.10, 4 is a sextic residue modulo p. That is there exists an integer x such that $x^6 \equiv 4 \pmod p$ which implies that $(x^3)^2 \equiv 2^2 \pmod p$. Thus in view of Lemma 6.8, 2 is a cubic residue modulo p. □

In view of the above results, we have the following result.

Theorem 6.12. *4 is a sextic residue modulo $p \equiv 1 \pmod 6$ if and only if $p = x^2 + 27y^2$.*

Our next two results provide some sufficient conditions for a prime $p = x^2 + 27y^2$ to be of the form $8k \pm 3$.

Theorem 6.13. *If $p = x^2 + 27y^2$ is a prime, where $x = \begin{cases} 6l + 2, & \text{if } l \text{ is odd,} \\ 6l + 4, & \text{if } l \text{ is even} \end{cases}$ and y is an odd integer. Then $p \equiv 3 \pmod 8$ and $p \equiv 1 \pmod 6$.*

Proof. Let $x = 6l + 2$, where l is odd and $y = 2m + 1$. Then, $p = (6l + 2)^2 + 27(2m+1)^2 \equiv 4l^2 + 4 + 3 \pmod 8$. Since $l^2 \equiv 1 \pmod 8$, therefore $p \equiv 3 \pmod 8$. Further $p = (6l + 2)^2 + 27(2m + 1)^2 \equiv 1 \pmod 6$. Similarly, if $x = 6l + 4$, where l is even, and y is an odd integer. Then $p \equiv 3 \pmod 8$ and $p \equiv 1 \pmod 6$.

Similarly, we can have the following theorem. □

Theorem 6.14. *If* $p = x^2+27y^2$ *is a prime, where* $y = \begin{cases} 6l+2, & \text{if } l \text{ is even,} \\ 6l+4, & \text{if } l \text{ is odd} \end{cases}$ *and* $x \equiv 1$ *or* $5 \pmod 6$. *Then* $p \equiv -3 \pmod 8$ *and* $p \equiv 1 \pmod 6$.

In view of Theorems 6.7, 6.12, 6.13 and 6.14, we have the following result.

Theorem 6.15. *Let* $p = 6f + 1$. *Then there are cyclotomic* Q *codes of length* p *which are not quaternary QR codes if and only if one of the following two sets of conditions is satisfied*:

$\begin{cases} p \equiv 13 \pmod{48} \\ p = x^2 + 27y^2 \quad \text{for some } x, y, \end{cases}$ $\begin{cases} p \equiv 19 \pmod{24} \\ p = x^2 + 27y^2 \quad \text{for some } x, y. \end{cases}$

We now present the primes $p < 10000$ which satisfy either of the condition given in Theorem 6.15 and thus for which cyclocotomic Q codes of order 6 exist:

(i) p = 43, 283, 307, 499, 643, 691, 739, 811, 1051, 1339, 1459, 1579, 1627, 1699, 2179, 2203, 2251, 2731, 3163, 3331, 4339, 4651, 6091, 6427, 6451, 7867, 8059, 8419, 8419, 9811. Here $p \equiv 19 \pmod{24}$ and $p = x^2 + 27y^2$.

(ii) p = 109, 157, 229, 277, 397, 733, 1069, 1789, 2749, 2917, 3061, 3229, 3541, 4597, 4909, 5101, 5413, 5437, 5653, 5821, 6037, 6133, 6661, 6997, 7333, 7741, 8101, 8317, 8389, 8629, 8941, 9013, 9133, 9781. Here $p \equiv 13 \pmod{48}$ and $p = x^2 + 27y^2$.

H. Tada et al. [29] proved the conjecture of Ding and Pless [12] which states that there are infinitely many primes p such that there are binary cyclotomic duadic codes of prime length p and order $2e$ with $e \geq 2$ that are not quadratic residue codes. Using the results in [12,29] we can also give partial answer to the question that whether there are infinitely many primes p such that there are cyclotomic Q codes of prime length p and order e at least for $e = 6$ that are not quaternary/binary quadratic residue codes. For this we recall the definition of $Spl\{f(x)\}$ (for detail see [29, p. 11]) given below:

Let $f(x)$ be a monic irreducible polynomial with integer coefficients. Reducing the coefficients of $f(x)$ modulo p, we obtain a polynomial $f_p(x)$ with coefficients in F_p. We define $Spl\{f(x)\}$ to be the set of primes such that $f_p(x)$ factors into a set of distinct linear polynomials over F_p. Using this definition we can rephrase Theorem 6.15 as follows:

Theorem 6.16. *Let* $p = 6f + 1$. *Then there are cyclotomic* Q *codes of length* p *which are not quaternary QR codes if and only if* $p \in Spl\{x^3 - 4\}$ *and* $p \notin Spl\{x^2 - 2\}$.

Now as discussed in [29]*, it can be easily seen that there are infinitely many primes p such that $p \in Spl\{x^3 - 4\}$. Further, there are infinitely many primes p of the form $8k \pm 3$, i.e., $p \notin Spl\{x^2 - 2\}$. However, it is to be seen whether there are infinitely many primes p such that $p \in Spl\{x^3 - 4\}$ as well as $p \notin Spl\{x^2 - 2\}$.*

Conclusions.

1. Parity of cyclotomic numbers of order 2, 4 and 6 associated with 4-cyclotomic cosets modulo an odd prime p are obtained. In our subsequent paper, we will obtain parity of cyclotomic numbers of order 8 and 12.
2. Unlike the approach used in [25] we either need not to find cyclotomic numbers or have to find a few of them to obtain the primitive idempotents of minimal cyclic codes of length p^n over F_4 for various primes p.
3. Some orthogonal properties of the above codes are discussed.
4. We also show that a Q code of prime length is always cyclotomic like a binary duadic code of prime length.
5. We have succeeded partially to answer the question - Whether there exist infinite number of primes p such that there are cyclotomic Q codes of length p and order 6 that are not binary/quaternary QR codes like cyclotomic binary duadic codes of length p and order 6 other than binary QR codes. Further in support of our claim, a number of primes less than 10000 for which cyclotomic Q codes of order 6 exist have been listed.
6. Using the approach discussed in the paper, we can obtain primitive idempotents in the semisimple ring $F_{2^k}[x]/\langle x^{p^n} - 1\rangle$ for any odd prime p and $k \geq 1$.

References

[1] S. K. Arora, S. Batra, and S. D. Cohen, *The primitive idempotents of a cyclic group algebra. II*, Southeast Asian Bull. Math. **29** (2005), no. 2, 197–208.

[2] S. K. Arora, S. Batra, S. D. Cohen, and M. Pruthi, *The primitive idempotents of a cyclic group algebra*, Southeast Asian Bull. Math. **26** (2002), no. 4, 549–557.

[3] S. K. Arora and M. Pruthi, *Minimal cyclic codes of length $2p^n$*, Finite Fields Appl. **5** (1999), no. 2, 177–187.

[4] G. K. Bakshi and M. Raka, *Minimal cyclic codes of length 2^m*, Ranchi Univ. Math. J. **33** (2002), 1–18 (2003).

[5] ———, *Minimal cyclic codes of length $p^n q$*, Finite Fields Appl. **9** (2003), no. 4, 432–448.

[6] S. Batra and S. K. Arora, *Minimal quadratic residue cyclic codes of length p^n (p odd prime)*, Korean J. Comput. Appl. Math. **8** (2001), no. 3, 531–547.

[7] ———, *Minimal quadratic residue cyclic codes of length 2^n*, J. Appl. Math. Comput. **18** (2005), no. 1-2, 25–43.

[8] ———, *Some cyclic codes of length $2p^n$*, Des. Codes Cryptogr. **61** (2011), no. 1, 41–69.

[9] David M. Burton, *Elementary Number Theory*, (Tata McGraw-Hill Publishers, New Delhi, 2007)

[10] B. Chen, H. Liu, and G. Zhang, *Some minimal cyclic codes over finite fields*, Discrete Math. **331** (2014), 142–150.
[11] ———, *A class of minimal cyclic codes over finite fields*, Des. Codes Cryptogr. **74** (2015), no. 2, 285–300.
[12] C. Ding and V. Pless, *Cyclotomy and duadic codes of prime lengths*, IEEE Trans. Inform. Theory **45** (1999), no. 2, 453–466.
[13] K. Ding and C. Ding, *A class of two-weight and three-weight codes and their applications in secret sharing*, IEEE Trans. Inform. Theory **61** (2015), no. 11, 5835–5842.
[14] R. A. Ferraz and C. Polcino Milies, *Idempotents in group algebras and minimal abelian codes*, Finite Fields Appl. **13** (2007), no. 2, 382–393.
[15] P. Kumar and S. K. Arora, *λ-mapping and primitive idempotents in semisimple ring* R_m, Comm. Algebra **41** (2013), no. 10, 3679–3694.
[16] P. Kumar, S. K. Arora, and S. Batra, *Primitive idempotents and generator polynomials of some minimal cyclic codes of length $p^n q^m$*, Int. J. Inf. Coding Theory **2** (2014), no. 4, 191–217.
[17] J. S. Leon, J. M. Masley, and V. Pless, *Duadic codes*, IEEE Trans. Inform. Theory **30** (1984), no. 5, 709–714.
[18] F. Li, Q. Yue, and C. Li, *Irreducible cyclic codes of length $4p^n$ and $8p^n$*, Finite Fields Appl. **34** (2015), 208–234.
[19] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes. I*, North-Holland Publishing Co., Amsterdam, 1977.
[20] V. Pless, *Introduction to the Theory of Error-Correcting Codes*, John Wiley & Sons, Inc., New York, 1982.
[21] ———, *Q-codes*, J. Combin. Theory Ser. A **43** (1986), no. 2, 258–276.
[22] M. Pruthi, *Cyclic codes of length 2^m*, Proc. Indian Acad. Sci. Math. Sci. **111** (2001), no. 4, 371–379.
[23] M. Pruthi and S. K. Arora, *Minimal codes of prime-power length*, Finite Fields Appl. **3** (1997), no. 2, 99–113.
[24] S. Rani, I. Singh, and S. K. Arora, *Primitive idempotents of irreducible cyclic codes of length $p^n q^m$*, Far East J. Math. **77** (2013), no. 1, 17–32.
[25] A. Sharma, Gurmeet K. Bakshi, V. C. Dumir, and M. Raka, *Cyclotomic numbers and primitive idempotents in the ring* $\mathrm{GF}(q)[x]/(x^{p^n}-1)$, Finite Fields Appl. **10** (2004), no. 4, 653–673.
[26] J. Singh and S. K. Arora, *Minimal cyclic codes of length $8p^n$ over $GF(q)$, where q is prime power of the form $8k+5$*, J. Appl. Math. Comput. **48** (2015), no. 1-2, 55–69.
[27] K. Singh and S. K. Arora, *The primitive idempotents in FC_{2^n}—I*, Int. J. Algebra **4** (2010), no. 25-28, 1231–1241.
[28] T. Storer, *Cyclotomy and difference sets*, Lectures in Advanced Mathematics, No. 2, Markham Publishing Co., Chicago, IL, 1967.
[29] H. Tada, S. Nishimura, and T. Hiramatsu, *Cyclotomy and its application to duadic codes*, Finite Fields Appl. **16** (2010), no. 1, 4–13.
[30] A. J. van Zanten, A. Bojilov, and S. M. Dodunekov, *Generalized residue and t-residue codes and their idempotent generators*, Des. Codes Cryptogr. **75** (2015), no. 2, 315–334.

Sudhir Batra
Department of Mathematics
DCR University of Science and Technology
Murthal (Sonipat) - 131039, India
Email address: batrasudhir@rediffmail.com

Rekha Mathur
Department of Mathematics
DCR University of Science and Technology
Murthal (Sonipat) - 131039, India
Email address: rekhaiitd.mathur@gmail.com