International Journal of Algebra, Vol. 5, 2011, no. 6, 285 - 294

Primitive Idempotents of Irreducible Quadratic Residue Cyclic Codes of Length $p^n q^m$

Ranjeet Singh

Department of Mathematics, M.D.University, Rohtak-124001, India
bharranjeet@yahoo.com

Manju Pruthi

Department of Mathematics, MDUPGRC Rewari 123401 (Haryana) India

Abstract

Explicit expressions for all the 4mn+2n+2m+1 primitive idempotents in the ring $R_{p^n q^m} = GF(l)[x]/(x^{p^n q^m} - 1)$, where p, q, l are distinct odd primes $o(l)_{p^n} = \phi(p^n)/2$,(n ≥ 1) and $o(l)_{q^m} = \phi(q^m)/2, (m \geq 1)$ with gcd($\phi(p^n)/2, \phi(q^m)/2$)=1, are obtained.

Mathematical Subject Classification: 20C05, 94B05, 16S34

Keywords: primitive idempotents; primitive root; cyclotomic cosets

1. Introduction

Let GF(l) be a field of odd prime order l. Let $\eta \geq 1$ be an integer with gcd(l, η)=1. Let $R_\eta = GF(l)[x]/(x^\eta - 1)$. The minimal cyclic codes of length η over GF(l) are the ideals of the ring R_η generated by the primitive idempotents. For $\eta = 2$, 4, p^n, $2p^n$, p an odd prime and l *is* primitive root mod(η) the primitive idempotent in R_η have been obtained by Arora and Pruthi [1,2] .When $m = p^n q$ where p, q are distinct odd primes and l is a primitive root mod p^n and q both with gcd ($\phi(p^n)/2$, $\phi(q)/2$) = 1, the primitive idempotent in R_η have been obtained by, G.K.Bakshi and Madhu Raka [4]. In this paper, we consider the case when $\eta = p^n q^m$ where p, q are distinct odd primes $o(l)_{p^n} = \phi(p^n)/2$, (n ≥ 1) and $o(l)_{q^m} = \phi(q^m)/2, (m \geq 1)$ with gcd ($\phi(p^n)/2, \phi(q^m)/2$)=1.We obtain explicit expressions for all the 4mn+2n+2m+1 primitive idempotents in $R_{p^n q^m}$ (see Theorem 4.1).

2. Primitive idempotents in $R_{p^n q^m} = GF(l)[x]/(x^{p^n q^m} - 1)$

2.1. For $0 \leq s \leq \eta - 1$, let $C_s = \{s, sl, sl^2, ..., sl^{t_s - 1}\}$, where t_s is the least positive integer such that $sl^{t_s} \equiv s \pmod{\eta}$ be the cyclotomic coset containing s, if α denotes a primitive ηth root of unity in some extension field of GF(l) then the polynomial $M^s(x) = \prod_{i \in C_s}(x - \alpha^i)$ is the minimal polynomial of α^s over GF(l).Let M_s be the minimal ideal in R_η generated by $\dfrac{x^\eta - 1}{M^s(x)}$ and θ_s be the primitive idempotent of M_s then we know by (Theorem1, [4]) the primitive idempotent θ_s corresponding to the cyclotomic coset C_s containing s in $R_{p^n q^m}$ is given by $\theta_s = \sum_{i=0}^{p^n q^m - 1} \varepsilon_i x^i$ Where $\varepsilon_i = \dfrac{1}{p^n q^m} \sum_{j \in C_s} \alpha^{-ij}$ $\forall i \geq 0$ .Thus to describe θ_s it becomes necessary to compute ε_i .To compute ε_i numerically, we consider the case when – $C_1 = C_{ab}$ and we get that $\varepsilon_i = \dfrac{1}{p^n q^m} \sum_{j \in C_s} \alpha^{-ij} = \dfrac{1}{p^n q^m} \sum_{j \in C_{sab}} \alpha^{ij}$ $\forall i \geq 0$ Where a, b are defined in lemma2.2.

Lemma2.1. Let p, q, l be distinct odd primes and n ≥ 1, m ≥ 1 are integers, $o(l)_{p^n} = \dfrac{\phi(p^n)}{2}$, $o(l)_{q^m} = \dfrac{\phi(q^m)}{2}$ and $\gcd\left(\dfrac{\phi(p^n)}{2}, \dfrac{\phi(q^m)}{2}\right)$=1.Then $o(l)_{p^{n-j} q^{m-k}} = \dfrac{\phi(p^{n-j} q^{m-k})}{4}$, for all $0 \leq j \leq n-1, 0 \leq k \leq m-1$.

Proof . Trivial.

Lemma2.2. For given distinct odd primes p, q, l there always exists fixed integers a and b satisfying $(a, pql) = 1$, 1 < a < pq, a $\not\equiv l^t$ (mod pq), b $\not\equiv$ r l^t (mod pq), r=a or 1 for 0 ≤ t ≤ $\dfrac{\phi(pq)}{4} - 1$.Further, for 0 ≤ j ≤ n-1 and 0 ≤ k ≤ m-1, the set {1, l, l^2,

…, $l^{\frac{\phi(p^{n-j}q^{m-k})}{4}-1}$, a, a$l$, …, a$l^{\frac{\phi(p^{n-j}q^{m-k})}{4}-1}$,b, b$l$, b$l^2$, …,b $l^{\frac{\phi(p^{n-j}q^{m-k})}{4}-1}$, ab, ab$l$, …, ab$l^{\frac{\phi(p^{n-j}q^{m-k})}{4}-1}$}forms a reduced residue system (mod $p^{n-j}\ q^{m-k}$).

Proof . Trivial**.**

Remark2.1: Since in the above lemma2.2 we have a $\not\equiv l^k$ (modpq), and b $\not\equiv$rl^k (mod pq), where 0 ≤ k ≤ $\frac{\phi(pq)}{4}-1$ and r = a or 1, then mainly the following cases holds: For 0 ≤ s ≤ $\frac{\phi(pq)}{4}$ −1,we have

Case (i) a $\equiv l^s$ (mod p), b $\equiv l^s$ (mod q), b $\not\equiv l^s$ (mod p) and a $\not\equiv l^s$ (mod q)
Case (ii) a$\equiv l^s$ (mod q) , b$\equiv l^s$ (mod p) , b $\not\equiv l^s$ (mod q) and a $\not\equiv l^s$ (mod p)
Case (iii) a $\not\equiv l^s$ (mod p), b $\equiv l^s$ (mod q), b $\not\equiv l^s$ (mod p) and a $\not\equiv l^s$ (mod q)
Case (iv) a $\not\equiv l^s$ (mod p), a $\equiv l^s$ (mod q), b $\not\equiv l^s$ (mod p) and b $\not\equiv l^s$ (mod q)

Here we are considering the case (i) because the remaining cases follows in a similar way.

Theorem2.1. If η = p^nq^m (n, m ≥ 1), then the 4mn+2n+2m+1 cyclotomic cosets modulo p^nq^m are given by (i) C_0= {0}. For 0 ≤ j ≤ m−1, (ii) $C_{p^nq^j}$ = { p^nq^j, p^nq^j l, …, $p^nq^j\ l^{\frac{\phi(q^{m-j})}{2}-1}$}(iii) $C_{ap^nq^j}$ = {a p^nq^j, a p^nq^j l,… a $p^nq^j\ l^{\frac{\phi(q^{m-j})}{2}-1}$}.For 0 ≤ i ≤n−1,(iv) $C_{p^iq^m}$ = { p^iq^m, p^iq^m l, …, $p^iq^m\ l^{\frac{\phi(p^{n-i})}{2}-1}$},(v) $C_{bp^iq^m}$ = {b p^iq^m, b p^iq^m l, …, b $p^iq^m\ l^{\frac{\phi(p^{n-i})}{2}-1}$}.

(vi)For 0 ≤ i ≤n−1, 0 ≤ j ≤ m−1

$C_{p^iq^j}$ = { p^iq^j, p^iq^jl, …, $p^iq^j\ l^{\frac{\phi(p^{n-i}q^{m-j})}{4}-1}$},

(vii) $C_{ap^iq^j}$ = {a p^iq^j, a p^iq^jl, …,a $p^iq^j\ l^{\frac{\phi(p^{n-i}q^{m-j})}{4}-1}$}(viii)$C_{bp^iq^j}$ = {b p^iq^j, b p^iq^jl, …, b $p^iq^j\ l^{\frac{\phi(p^{n-i}q^{m-j})}{4}-1}$},(ix) $C_{abp^iq^j}$ = {ab p^iq^j, ab p^iq^jl, …,ab $p^iq^j\ l^{\frac{\phi(p^{n-i}q^{m-j})}{4}-1}$}, where a and b are defined in lemma2.2.

Proof.Trivial.

Remark2.2. Let α be a fixed primitive p^nq^mth root of unity in some extension field of$GF(l)$.For $0 \le i \le n-1,\ 0 \le j \le m-1$, define $A_{(i,j)} = \sum_{s\in C_b} \alpha^{p^i q^j s}$, $B_{(i,j)} = \sum_{s\in C_1} \alpha^{p^i q^j s}$, $Y_{(i,j)} = \sum_{s\in C_{ab}} \alpha^{p^i q^j s}$ $X_{(i,j)} = \sum_{s\in C_a} \alpha^{p^i q^j s}$,

$\eta_0 = \sum_{s=0}^{\frac{\phi(p)}{2}} (\alpha^{p^{n-1}q^m s})^{l^s}$, $\eta_1 = \sum_{s=0}^{\frac{\phi(p)}{2}} (\alpha^{p^{n-1}q^m s})^{bl^s}$, $\eta_0^* = \sum_{s=0}^{\frac{\phi(q)}{2}} (\alpha^{p^n q^{m-1} s})^{l^s}$

and $\eta_1^* = \sum_{s=0}^{\frac{\phi(q)}{2}} (\alpha^{p^n q^{m-1} s})^{al^s}$ As $C_l = C_1,\ C_{bl} = C_b, C_{al} = C_a, C_{abl} = C_{ab}$ and, it then follows that $(A_{(i,j)})^l = A_{(i,j)}$, $(B_{(i,j)})^l = B_{(i,j)}$ $(X_{(i,j)})^l = X_{(i,j)}$, $(Y_{(i,j)})^l = Y_{(i,j)}$, $(\eta_0)^l = \eta_0$, $(\eta_1)^l = \eta_1$, $(\eta_0^*)^l = \eta_0^*$, $(\eta_1^*)^l = \eta_1^*$ therefore, $A_{(i,j)}, B_{(i,j)}$, $X_{(i,j)}, Y_{(i,j)}$, η_0, η_1, η_0^*, $\eta_1^* \in$ GF(l).

3. Some lemmas

Lemma3.1. For $0 \le j \le n-1,\ 0 \le k \le m-1$, if β is primitive $p^j q^k$th root of unity in some extension field of $GF(l)$ and $\alpha(l)_{p^j q^k} = \frac{\phi(p^j q^k)}{4}$,then

$$\sum_{s=0}^{\frac{\phi(p^j q^k)}{4}-1} (\beta^{l^s} + \beta^{bl^s} + \beta^{al^s} + \beta^{abl^s}) = \begin{cases} 1 & if\ (j,k) = (1,1) \\ 0 & if\ (j,k) \ne (1,1) \end{cases}.$$

Proof. Trivial.

Lemma3.2. For $0 \le i \le n-1, 0 \le j \le m-1$.

$$A_{(i,j)} + B_{(i,j)} + X_{(i,j)} + Y_{(i,j)} = \begin{cases} p^{n-1}q^{m-1} & if\ (i,j) = (n-1, m-1) \\ 0 & if\ (i,j) \le (n-2, m-2) \end{cases}.$$

Proof. Trivial.

Lemma3.3. For $0 \le k \le m-1$,
$$\sum_{s\in C_{p^n q^k}} \alpha^{p^i q^r s} = \begin{cases} \eta_0^* q^{m-k-1} & if\ (r+k) = m-1 \\ 0 & if\ (r+k) < m-1 \\ \frac{\phi(q^{m-k})}{2} & if\ (r+k) \ge m \end{cases}$$

Proof. Trivial.

Lemma3.4. For $0 \le k \le m-1$,
$$\sum_{s\in C_{ap^n q^k}} \alpha^{p^i q^r s} = \begin{cases} \eta_1^* q^{m-k-1} & if\ (r+k) = m-1 \\ 0 & if\ (r+k) < m-1 \\ \frac{\phi(q^{m-k})}{2} & if\ (r+k) \ge m \end{cases}$$

Proof. Trivial.

Lemma3.5. For $0 \le j \le n-1$, $\sum_{s \in C_{p^j q^m}} \alpha^{p^i q^r s} = \begin{cases} \eta_0 p^{n-j-1} & if \quad (i+j) = n-1 \\ 0 & if \quad (i+j) < n-1 \\ \dfrac{\phi(p^{n-j})}{2} & if \quad (i+j) \ge n \end{cases}$

Proof. Trivial

Lemma3.6. For $0 \le j \le n-1$, $\sum_{s \in C_{bp^j q^m}} \alpha^{p^i q^r s} = \begin{cases} \eta_1 p^{n-j-1} & if \quad (i+j) = n-1 \\ 0 & if \quad (i+j) < n-1 \\ \dfrac{\phi\left(p^{n-j}\right)}{2} & if \quad (i+j) \ge n \end{cases}$

Proof. Trivial.

Lemma3.7. For $0 \le j \le n-1$ and $0 \le k \le m-1$

$$\sum_{s \in C_{bp^j q^k}} \alpha^{bp^i q^r s} = \sum_{s \in C_{p^j q^k}} \alpha^{p^i q^r s} = \sum_{s \in C_{ap^j q^k}} \alpha^{ap^i q^r s} = \sum_{s \in C_{abp^j q^k}} \alpha^{abp^i q^r s}$$

$$= \begin{cases} \dfrac{1}{p^j q^k} B_{(i+j, r+k)} & if \ (i+j) \le n-1 \ and \ (r+k) \le m-1 \\ \dfrac{\phi(p^{n-j}) q^{m-k-1}}{2} \eta_0^* & if \quad (i+j) \ge n \ and \ (r+k) = m-1 \\ 0 & if \quad (i+j) \ge n \ and \ (r+k) < m-1 \\ \dfrac{p^{n-j-1} \phi(q^{m-k})}{2} \eta_0 & if \quad (i+j) = n-1 \ and \ (r+k) \ge m \\ 0 & if \quad (i+j) < n-1 \ and \ (r+k) \ge m \\ \dfrac{\phi(p^{n-j} q^{m-k})}{4} & if \quad (i+j) \ge n \ and \ (r+k) \ge m \end{cases}.$$

Proof. Trivial.

Lemma3.8. For $0 \le j \le n-1, 0 \le k \le m-1$

$$\sum_{s \in C_{bp^j q^k}} \alpha^{p^i q^r s} = \sum_{s \in C_{p^j q^k}} \alpha^{bp^i q^r s} = \sum_{s \in C_{ap^j q^k}} \alpha^{abp^i q^r s} = \sum_{s \in C_{abp^j q^k}} \alpha^{ap^i q^r s}$$

$$= \begin{cases} \dfrac{1}{p^j q^k} A_{(i+j, r+k)} & if \ (i+j) \le n-1 \ and \ (r+k) \le m-1 \\ \dfrac{\phi(p^{n-j}) q^{m-k-1}}{2} \eta_0^* & if \quad (i+j) \ge n \ and \ (r+k) = m-1 \\ 0 & if \quad (i+j) \ge n \ and \ (r+k) < m-1 \\ p^{n-j-1} \dfrac{\phi(q^{m-k})}{2} \eta_1 & if \quad (i+j) = n-1 \ and \ (r+k) \ge m \\ 0 & if \quad (i+j) < n-1 \ and \ (r+k) \ge m \\ \dfrac{\phi(p^{n-j} q^{m-k})}{4} & if \quad (i+j) \ge n \ and \ (r+k) \ge m \end{cases}$$

Proof. Trivial

Lemma3.9. For $0 \le j \le n-1, 0 \le k \le m-1$

$$\sum_{s\in C_{apjq^k}}\alpha^{p^iq^rs}=\sum_{s\in C_{abp^jq^k}}\alpha^{bp^iq^rs}=\sum_{s\in C_{p^jq^k}}\alpha^{ap^iq^rs}=\sum_{s\in C_{bp^jq^k}}\alpha^{abp^iq^rs}$$

$$=\begin{cases}\dfrac{1}{p^jq^k}X_{(i+j,r+k)} & \text{if } (i+j)\le n-1 \text{ and } (r+k)\le m-1\\ \dfrac{\phi(p^{n-j})q^{m-k-1}}{2}\eta_1^* & \text{if } (i+j)\ge n \text{ and } (r+k)=m-1\\ 0 & \text{if } (i+j)\ge n \text{ and } (r+k)<m-1\\ \dfrac{p^{n-j-1}\phi(q^{m-k})}{2}\eta_0 & \text{if } (i+j)=n-1 \text{ and } (r+k)\ge m\\ 0 & \text{if } (i+j)<n-1 \text{ and } (r+k)\ge m\\ \dfrac{\phi(p^{n-j}q^{m-k})}{4} & \text{if } (i+j)\ge n \text{ and } (r+k)\ge m\end{cases}$$

Proof. Trivial.

Lemma3.10. For $0\le j\le n-1, 0\le k\le m-1$

$$\sum_{s\in C_{abp^jq^k}}\alpha^{p^iq^rs}=\sum_{s\in C_{ap^jq^k}}\alpha^{bp^iq^rs}=\sum_{s\in C_{p^jq^k}}\alpha^{abp^iq^rs}=\sum_{s\in C_{bp^jq^k}}\alpha^{ap^iq^rs}$$

$$=\begin{cases}\dfrac{1}{p^jq^k}Y_{(i+j,r+k)} & \text{if } (i+j)\le n-1 \text{ and } (r+k)\le m-1\\ \dfrac{\phi(p^{n-j})q^{m-k-1}}{2}\eta_1^* & \text{if } (i+j)\ge n \text{ and } (r+k)=m-1\\ 0 & \text{if } (i+j)\ge n \text{ and } (r+k)<m-1\\ p^{n-j-1}\dfrac{\phi(q^{m-k})}{2}\eta_1 & \text{if } (i+j)=n-1 \text{ and } (r+k)\ge m\\ 0 & \text{if } (i+j)<n-1 \text{ and } (r+k)\ge m\\ \dfrac{\phi(p^{n-j}q^{m-k})}{4} & \text{if } (i+j)\ge n \text{ and } (r+k)\ge m\end{cases}.$$

Proof. Trivial.

4. Main Result

Theorem4.1. The 4mn+2n+2m+1 primitive idempotents in $R_{p^nq^m}$ are given by

(i) $\theta_0(x)=\dfrac{1}{p^nq^m}(1+x+x^2+\ldots+x^{p^nq^m-1})$.

(ii) For $0\le k\le m-1$,

$$\theta_{p^nq^k}(x)=\frac{1}{2p^nq^m}\{\phi(q^{m-k})[1+\sum_{(i,r)=(0,m-k)}^{(n-1,m-1)}(\sigma_{(i,r)}(x)+\sigma_{b(i,r)}(x)+\sigma_{a(i,r)}(x)+\sigma_{ab(i,r)}(x))$$

$$+\sum_{(i,r)=(n,m-k)}^{(n,m-1)}\sigma_{(n,r)}(x)+\sigma_{a(n,r)}(x)+\sum_{(i,r)=(0,m)}^{(n-1,m)}(\sigma_{(i,r)}(x)+\sigma_{b(i,r)}(x))]$$

$$+2\,q^{\text{m-k-1}}\ [\sum_{i=0}^{n-1}\eta_1^*(\sigma_{(i,m-k-1)}(x)+\sigma_{b(i,m-k-1)}(x))+\eta_0^*(\sigma_{a(i,m-k-1)}(x)+\sigma_{ab(i,m-k-1)}(x))$$

$$+\eta_1^*(\sigma_{(n,m-k-1)}(x))+\eta_0^*(\sigma_{a(n,m-k-1)}(x))]\}.$$

(iii) For $0\le k\le m-1$

$$\theta_{ap^nq^k}(x)=\frac{1}{2p^nq^m}\{\ \phi(q^{m-k})[1+\sum_{(i,r)=(0,m-k)}^{(n-1,m-1)}(\sigma_{(i,r)}(x)+\sigma_{b(i,r)}(x)+\sigma_{a(i,r)}(x)+\sigma_{ab(i,r)}(x))$$

$$+\sum_{(i,r)=(n,m-k)}^{(n,m-1)}\sigma_{(n,r)}(x)+\sigma_{a(n,r)}(x)+\sum_{(i,r)=(0,m)}^{(n-1,m)}(\sigma_{(i,r)}(x)+\sigma_{b(i,r)}(x))]$$

$$+2\,q^{\text{m-k-1}}\ [\sum_{i=0}^{n-1}\eta_0^*(\sigma_{(i,m-k-1)}(x)+\sigma_{b(i,m-k-1)}(x))+\eta_1^*(\sigma_{a(i,m-k-1)}(x)+\sigma_{ab(i,m-k-1)}(x))$$

$$+\eta_0^*(\sigma_{(n,m-k-1)}(x))+\eta_1^*(\sigma_{a(n,m-k-1)}(x))]\}.$$

(iv) For $0\le j\le n-1$

$$\theta_{p^jq^m}(x)=\frac{1}{p^nq^m}\{$$

$$p^{n-j-1}\sum_{r=0}^{m-1}\{\eta_1(\sigma_{(n-j-1,r)}(x)+\sigma_{a(n-j-1,r)}(x))+\eta_0(\sigma_{b(n-j-1,r)}(x)+\sigma_{ab(n-j-1,r)}(x))\}+$$

$$\frac{\phi(p^{n-j})}{2}\sum_{r=0}^{m}\sigma_{(n,r)}(x)+\sigma_{a(n,r)}(x)+$$

$$\frac{\phi(p^{n-j})}{2}\sum_{(i,r)=(n-j,0)}^{(n-1,m-1)}(\sigma_{(i,r)}(x)+\sigma_{b(i,r)}(x)+\sigma_{a(i,r)}(x)+\sigma_{ab(i,r)}(x)$$

$$+\ p^{n-j-1}(\eta_1\sigma_{(i,m)}(x)+\eta_0\sigma_{b(i,m)}(x))+\frac{\phi(p^{n-j})}{2}\sum_{i=n-j}^{n-1}(\sigma_{(i,m)}(x)+\sigma_{b(i,m)}(x))\}.$$

(v) For $0\le j\le n-1$

$$\theta_{bp^jq^m}(x)=\frac{1}{p^nq^m}\{$$

$$p^{n-j-1}\sum_{r=0}^{m-1}\{\eta_0(\sigma_{(n-j-1,r)}(x)+\sigma_{a(n-j-1,r)}(x))+\eta_1(\sigma_{b(n-j-1,r)}(x)+\sigma_{ab(n-j-1,r)}(x))\}+$$

$$\frac{\phi(p^{n-j})}{2}\sum_{r=0}^{m}\sigma_{(n,r)}(x)+\sigma_{a(n,r)}(x)+$$

$$\frac{\phi(p^{n-j})}{2}\sum_{(i,r)=(n-j,0)}^{(n-1,m-1)}(\sigma_{(i,r)}(x)+\sigma_{b(i,r)}(x)+\sigma_{a(i,r)}(x)+\sigma_{ab(i,r)}(x)$$

$$+\ p^{n-j-1}(\eta_0\sigma_{(i,m)}(x)+\eta_1\sigma_{b(i,m)}(x))+\frac{\phi(p^{n-j})}{2}\sum_{i=n-j}^{n-1}(\sigma_{(i,m)}(x)+\sigma_{b(i,m)}(x))\}.$$

(vi) For $0\le j\le$ n-1 and $0\le k\le$ m-1,

$$\theta_{p^jq^k}(x)=\frac{1}{p^nq^m}\{\frac{1}{p^jq^k}\sum_{(i,r)=(0,0)}^{(n-j-1,m-k-1)}[A_{(i+j,r+k)}\sigma_{a(i,r)}(x)+B_{(i+j,r+k)}\sigma_{ab(i,r)}(x)]$$

$$+\frac{1}{p^j q^k}\sum_{(i,r)=(0,0)}^{(n-j-1,m-k-1)}[X_{(i+j,r+k)}\sigma_{b(i,r)}(x)+Y_{(i+j,r+k)}\sigma_{(i,r)}(x)]$$

$$+\frac{\phi(p^{n-j})q^{m-k-1}}{2}[\sum_{(i,r)=(n-j,m-k-1)}^{(n-1,m-k-1)}\{\eta_0^*(\sigma_{a(i,m-k-1)}(x)+\sigma_{ab(i,m-k-1)}(x))+\eta_1^*(\sigma_{(i,m-k-1)}(x)+\sigma_{b(i,m-k-1)}(x))\}$$

$$+\eta_1^*\ \sigma_{(n,m-k-1)}(x)+\eta_0^*\ \sigma_{a(n,m-k-1)}(x)\ ]$$

$$+\ p^{n-j-1}\frac{\phi(q^{m-k})}{2}\sum_{(i,r)=(n-j-1,m-k)}^{(n-j-1,m)}[\eta_1(\sigma_{(n-j-1,r)}(x)+\sigma_{a(n-j-1,r)}(x))+\eta_o(\sigma_{b(n-j-1,r)}(x)+\sigma_{ab(n-j-1,r)}(x))]$$

$$+\frac{\phi(p^{n-j}q^{m-k})}{4}[\sum_{(i,r)=(n-j,m-k)}^{(n-1,m-1)}(\sigma_{(i,,r)}(x)+\sigma_{b(i,r)}(x)+\sigma_{a(i,,r)}(x)+\sigma_{ab(i,r)}(x))$$

$$+\sum_{(i,r)=(n,m-k)}^{(n,m-1)}\sigma_{(n,,r)}(x)+\sigma_{a(n,,r)}(x)\ +\sum_{(i,r)=(n-j,m)}^{(n-1,m)}(\sigma_{(i,m)}(x)+\sigma_{b(i,m)}(x)\ )+1]\}.$$

$$\text{(vii)}\ \theta_{bp^jq^k}(x)=\frac{1}{p^nq^m}\ \{\frac{1}{p^jq^k}\sum_{(i,r)=(0,0)}^{(n-j-1,m-k-1)}[B_{(i+j,r+k)}\sigma_{a(i,r)}(x)+A_{(i+j,r+k)}\sigma_{ab(i,r)}(x)]$$

$$+\frac{1}{p^jq^k}\sum_{(i,r)=(0,0)}^{(n-j-1,m-k-1)}[Y_{(i+j,r+k)}\sigma_{b(i,r)}(x)+X_{(i+j,r+k)}\sigma_{(i,r)}(x)]+$$

$$\frac{\phi(p^{n-j})q^{m-k-1}}{2}[\sum_{(i,r)=(n-j,m-k-1)}^{(n-1,m-k-1)}\{\eta_0^*(\sigma_{a(i,m-k-1)}(x)+\sigma_{ab(i,m-k-1)}(x))+\eta_1^*(\sigma_{(i,m-k-1)}(x)+\sigma_{b(i,m-k-1)}(x))\}$$

$$+\eta_1^*\ \sigma_{(n,m-k-1)}(x)+\eta_0^*\ \sigma_{a(n,m-k-1)}(x)\ ]+$$

$$p^{n-j-1}\frac{\phi(q^{m-k})}{2}\sum_{(i,r)=(n-j-1,m-k)}^{(n-j-1,m)}[\eta_0(\sigma_{(n-j-1,r)}(x)+\sigma_{a(n-j-1,r)}(x))+\eta_1(\sigma_{b(n-j-1,r)}(x)+\sigma_{ab(n-j-1,r)}(x))]$$

$$+\frac{\phi(p^{n-j}q^{m-k})}{4}[\sum_{(i,r)=(n-j,m-k)}^{(n-1,m-1)}(\sigma_{(i,,r)}(x)+\sigma_{b(i,r)}(x)+\sigma_{a(i,,r)}(x)+\sigma_{ab(i,r)}(x))$$

$$+\sum_{(i,r)=(n,m-k)}^{(n,m-1)}\sigma_{(n,,r)}(x)+\sigma_{a(n,,r)}(x)+\sum_{(i,r)=(n-j,m)}^{(n-1,m)}(\sigma_{(i,m)}(x)+\sigma_{b(i,m)}(x)\ )+1]\}\ .$$

$$\text{(viii)}\ \theta_{ap^jq^k}(x)=\frac{1}{p^nq^m}\ \{\frac{1}{p^jq^k}\sum_{(i,r)=(0,0)}^{(n-j-1,m-k-1)}[Y_{(i+j,r+k)}\sigma_{a(i,r)}(x)+X_{(i+j,r+k)}\sigma_{ab(i,r)}(x)]$$

$$+\frac{1}{p^jq^k}\sum_{(i,r)=(0,0)}^{(n-j-1,m-k-1)}[B_{(i+j,r+k)}\sigma_{b(i,r)}(x)+A_{(i+j,r+k)}\sigma_{(i,r)}(x)]+$$

$$\frac{\phi(p^{n-j})q^{m-k-1}}{2}[\sum_{(i,r)=(n-j,m-k-1)}^{(n-1,m-k-1)}\{\eta_1^*(\sigma_{a(i,m-k-1)}(x)+\sigma_{ab(i,m-k-1)}(x))+\eta_0^*(\sigma_{(i,m-k-1)}(x)+\sigma_{b(i,m-k-1)}(x))\}$$

$$+\eta_0^*\ \sigma_{(n,m-k-1)}(x)+\eta_1^*\ \sigma_{a(n,m-k-1)}(x)\ ]+$$

$$p^{n-j-1}\frac{\phi(q^{m-k})}{2}\sum_{(i,r)=(n-j-1,m-k)}^{(n-j-1,m)}[\eta_1(\sigma_{(n-j-1,r)}(x)+\sigma_{a(n-j-1,r)}(x))+\eta_o(\sigma_{b(n-j-1,r)}(x)+\sigma_{ab(n-j-1,r)}(x))]$$

$$+\frac{\phi(p^{n-j}q^{m-k})}{4}[\sum_{(i,r)=(n-j,m-k)}^{(n-1,m-1)}(\sigma_{(i,,r)}(x)+\sigma_{b(i,r)}(x)+\sigma_{a(i,,r)}(x)+\sigma_{ab(i,r)}(x))$$

$$+\sum_{(i,r)=(n,m-k)}^{(n,m-1)} \sigma_{(n,,r)}(x)+\sigma_{a(n,,r)}(x)+\sum_{(i,r)=(n-j,m)}^{(n-1,m)}(\sigma_{(i,m)}(x)+\sigma_{b(i,m)}(x))+1]\}.$$

(ix) $$\theta_{abp^j q^k}(x)=\frac{1}{p^n q^m}\{\frac{1}{p^j q^k}\sum_{(i,r)=(0,0)}^{(n-j-1,m-k-1)}[X_{(i+j,r+k)}\sigma_{a(i,r)}(x)+Y_{(i+j,r+k)}\sigma_{ab(i,r)}(x)]$$

$$+\frac{1}{p^j q^k}\sum_{(i,r)=(0,0)}^{(n-j-1,m-k-1)}[A_{(i+j,r+k)}\sigma_{b(i,r)}(x)+B_{(i+j,r+k)}\sigma_{(i,r)}(x)]$$

$$+\frac{\phi(p^{n-j})q^{m-k-1}}{2}[\sum_{(i,r)=(n-j,m-k-1)}^{(n-1,m-k-1)}\{\eta_1^*(\sigma_{a(i,m-k-1)}(x)+\sigma_{ab(i,m-k-1)}(x))+\eta_0^*(\sigma_{(i,m-k-1)}(x)+\sigma_{b(i,m-k-1)}(x))\}$$

$$+\eta_0^*\,\sigma_{(n,m-k-1)}(x)+\eta_1^*\,\sigma_{a(n,m-k-1)}(x)]+$$

$$p^{n-j-1}\frac{\phi(q^{m-k})}{2}\sum_{(i,r)=(n-j-1,m-k)}^{(n-j-1,m)}[\eta_0(\sigma_{(n-j-1,r)}(x)+\sigma_{a(n-j-1,r)}(x))+\eta_1(\sigma_{b(n-j-1,r)}(x)+\sigma_{ab(n-j-1,r)}(x))]$$

$$+\frac{\phi(p^{n-j}q^{m-k})}{4}[\sum_{(i,r)=(n-j,m-k)}^{(n-1,m-1)}(\sigma_{(i,,r)}(x)+\sigma_{b(i,r)}(x)+\sigma_{a(i,,r)}(x)+\sigma_{ab(i,r)}(x))$$

$$+\sum_{(i,r)=(n,m-k)}^{(n,m-1)}\sigma_{(n,,r)}(x)+\sigma_{a(n,,r)}(x)+\sum_{(i,r)=(n-j,m)}^{(n-1,m)}(\sigma_{(i,m)}(x)+\sigma_{b(i,m)}(x))+1]\}.$$

Where $A_{(n-1,m-1)} = p^{n-1}q^{m-1}(\frac{1+r+\gamma+\delta}{4})$, $B_{(n-1,m-1)} = p^{n-1}q^{m-1}(\frac{1+r-\delta-\gamma}{4})$

$X_{(n-1,m-1)} = p^{n-1}q^{m-1}(\frac{1-r-\gamma+\delta}{4})$, $Y_{(n-1,m-1)} = p^{n-1}q^{m-1}(\frac{1-r+\gamma-\delta}{4})$,

$\eta_0=\frac{-1+\sqrt{-p}}{2}$, $\eta_1=\frac{-1-\sqrt{-p}}{2}$, $\eta_o^*=\frac{-1+\sqrt{-q}}{2}$, $\eta_1^*=\frac{-1-\sqrt{-q}}{2}$, r^2=-q, γ^2=-p, δ^2=pq.

Proof. By repeated application of the lemma's defined above we get the required results for the primitive idempotents.

References

[1] S.K. Arora, M. Pruthi, Minimal cyclic codes of prime power length, Finite Fields Appl. 3 (1997)99-113.

[2] S.K. Arora, M. Pruthi, Minimal cyclic codes of length $2p^n$, Finite Fields Appl. 5 (1999) 177-187.

[3] Anuradha Sharma, G.K.Bakshi, V.C. Dumir, M. Raka, Cyclotomic Numbers and Primitive idempotents in the ring GF (l) [x]/<$x^{p^n}-1$>, Finite Fields Appl. 10 (2004) 653-673.

[4] G.K.Bakshi, Madhu Raka, Minimal cyclic codes of length $p^n q$, Finite Fields Appl. 9 (2003) 432-448.

[5] M. Pruthi, Cyclic codes of length 2^m, Proc. Indian Acad. Sci. 111 (2001) 371-379.

Received: September, 2010