Journal of Advances and Scholarly Researches in Allied Education

Vol. VII, Issue No. XIII, January-2014, ISSN 2230-7540

REVIEW ARTICLE

A STUDY ON MINIMAL CYCLIC CODES OF LENGTH $P^N Q$

Journal of Advances and Scholarly Researches in Allied Education
Vol. VII, Issue No. XIII, January-2014, ISSN 2230-7540

A Study on Minimal Cyclic Codes of Length p^nq

Manjeet Singh[1]* Dr. Pradeep Goel[2]

[1] Research Scholar, Department of Mathematics, Sai Nath University, Ranchi, Jharkhand

[2] Professor, M. M. College, Fatehabad, Haryana

Abstract – We aim at the circle $R_{p^nq} = GF(\ell)[x]/(x^{p^nq}-1)$ ***, If p, q, are separate odd primes, both pn and q are a primitive root.. Explicit terminology for the entire*** $(d+1)n+2$ ***Early idempotents are acquired,*** $d = gcd(\phi(p^n), \phi(q)),\ p \nmid (q-1)$ ***Dimensions and distances created by polynomials are discussed as well as minimum cyclic length codes pnq over*** $GF(\ell)$***.***

Key Words: Minimal Cyclic Codes , Cyclotomic Cosets

-----------------------------------x--------------------------------

INTRODUCATION

Let $GF(\ell)$ be a field of prime order ℓ, ℓ, odd. Let $m \geqslant 1$ be an integer with $gcd(\ell, m) = 1$. Let $R_m = GF(\ell)[x]/(x^m-1)$. Minimum m length cyclic codes $GF(\ell)$ are ideals of the ring R_m generated by the primitive idempotents. Arora and Pruthi [1,5] obtained the primitive idempotents in R_m for $m = 2, 4, p^n$ and $2p^n$ where p is an odd prime and ℓ The original root mod m. Pruthi [6] had a few idempotents $R_{2^n},\ n \geqslant 3.$. A. In both the first-name and lowly cyclic codes Sharma, G.K. Bakshi, V.C. Madhu Raka and Dumir [7] include $R_{2^n},\ n \geqslant 3.$. Madhu Raka and G.K. Bakshi [2] minimum cyclic duration codes were also obtained p^nq, q are various odd primes where p is, ℓ is a primitive root mod p^n and q both and $gcd(\phi(p^n), \phi(q)) = 2$. Manju Pruthi and Ranjeet Singh [8] The initial idempotents were contained in the ring $R_{p^nq^m} = GF(\ell)[x]/(x^{p^nq^m}-1)$, wherever p, q, ℓ Are different weird benefits and $(\phi(p^n), \phi(q^m)) = 2,\ o(\ell)_{p^n} = \phi(p^n)/2$ and $o(\ell)_{q^m} = \phi(q^m)/2$.

In this paper, When we glance at the situation $m = p^nq$, q is a primitive root of the two modes, where p is a particular odd primes p^n and mod q and $gcd(\phi(p^n), \phi(q)) = d,\ d \geqslant 2$, with $p \nmid (q-1)$. Clearly, d is even. $(p = 5,\ q = 17,\ \ell = 3,\ d = 4$ is one such sequence for every n.) The primitive idempotents (d + 1) n + 2 are specifically represented in the R_{p^nq} There was a mistake (see Section 4). We discuss in this section the dimension, polynomials created and the minimum distance from the minimum cyclic codes of pnq length $GF(\ell)$. This complements the findings of G.K. The cases D = 2 consider Bakshi and Madhu Raka[2].

PRIMITIVE IDEMPOTENTS IN $GF(\ell)[x]/(x^{p^nq}-1)$

Consider Mac Williams and Sloane [Theoremaccompanying]'s generalisation in the non-binary case

For $0 \leqslant s \leqslant m-1$, let $C_s = \{s, s\ell, s\ell^2, \ldots, s\ell^{m_s-1}\}$, where ms is such a small positive integer $s\ell^{m_s} \equiv s \pmod{m}$, Be the s-containing cyclotomic coset. If α is an early unification mth in an extension field $GF(\ell)$, then the polynomial $M^{(s)}(x) = \prod_{i\in C_s}(x-\alpha^i)$ is the minimal polynomial of α^s over $GF(\ell)$. Let $\mathcal{M}_s$ be the minimal ideal in R_m generated by $\frac{x^m-1}{M^{(s)}(x)}$ and $\theta_s(x)$ be the primitive idempotent of $\mathcal{M}_s$. We realise that then.

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

Theorem:
$\theta_s(x) = \sum_{i=0}^{m-1} \varepsilon_i x^i$ where $\varepsilon_i = \frac{1}{m}\sum_{j\in C_s}\alpha^{-ij}$ *for all* $i \geqslant 0$

Proof:

$$\sum_{j=0}^{m-1}\theta_s(\alpha^j)\alpha^{-ij} = \sum_{j=0}^{m-1}\sum_{k=0}^{m-1}\varepsilon_k\alpha^{jk}\alpha^{-ij} = \sum_{k=0}^{m-1}\varepsilon_k\sum_{j=0}^{m-1}\alpha^{j(k-i)} = m\varepsilon_i.$$

In spite of this (2.1),

$$\varepsilon_i = \frac{1}{m}\sum_{j=0}^{m-1}\theta_s(\alpha^j)\alpha^{-ij} = \frac{1}{m}\sum_{j\in C_s}\alpha^{-ij}$$

Recall that a decreased modulo φ(m) residue scheme consists of a collection of ̈a1,a2,...,aφ(m) $gcd(a_i, m) = 1$ and $a_i \neq a_j$ (mod m) for all $i, j,\ 1 \leqslant i, j \leqslant \phi(m),\ i \neq j$. The order of modulo m is the least positive integer h such that $\ell^h \equiv 1$ (mod m). If $h = \phi(m)$, The primitive root modulo m is then renamed. The primitive roots mod m only occur where it's well-known $m = 2, 4, p^e, 2p^e$ where p is an odd prime.

We took things for granted p, q, ℓ Are different weird benefits, $n \geqslant 1$ is an integer, an early root mod p^n and an original root mod q, $gcd(\phi(p^n), \phi(q)) = d \geqslant 2,\ p \nmid (q-1)$.

Lemma 1: If ℓ is an early root mod p^n, then ℓ is an early root mod p^{n-j} as well, for everyone $j, 0 \leqslant j \leqslant n-1$.

Proof: Madhu Raka and G.K. Bakshi [2, Lemma 1].

Lemma 2: Let p, q be distinct odd primes. Let ℓ be an integer such that $gcd(\ell, p^n q) = 1$. If belongs to exponent r, s,t modulo p^n, q and $p^n q$ respectively, then $t = lcm[r, s]$.

Proof: As $\ell^t \equiv 1 \pmod{p^n q}$, we get $\ell^t \equiv 1 \pmod{p^n}$ and $\ell^t \equiv 1 \pmod{q}$ so that $r \mid t$ and $s \mid t$. Consequently, $lcm[r, s] \mid t$. On the other hand, let $d = gcd(r, s)$. Then $\ell^r \equiv 1 \pmod{p^n}$ gives $\ell^{\frac{rs}{d}} \equiv 1 \pmod{p^n}$. Similarly, $\ell^s \equiv 1$ (mod q) gives $\ell^{\frac{s.r}{d}} \equiv 1$ (mod q). But p, q are distinct primes, so we get $\ell^{\frac{r.s}{d}} \equiv 1 \pmod{p^n q}$. However ℓ belongs to exponent t mod $p^n q$. Therefore, $t \mid \frac{rs}{d}$. Also $rs = gcd(r, s) \times lcm[r, s] = d \times lcm[r, s]$, i.e. $t \mid lcm[r, s]$. We thus conclude that $t = lcm[r, s]$.

Corollary 1: If is a primitive root mod p^n and also a primitive root mod q, then ℓ belongs to exponent $\frac{\phi(p^n q)}{d}$ mod $p^n q$, where $d = gcd(\phi(p^n), \phi(q))$.

Proof: By Lemma 2.

Corollary 2: Let p, q, ℓ be distinct primes, $n \geqslant 1$ be an integer, ℓ be a primitive root mod p^n as well as a primitive root mod q, where $gcd(\phi(p^n), \phi(q)) = d,\ p \nmid (q-1)$. Then the order of ℓ mod $p^{n-j}q$ is $\frac{\phi(p^{n-j}q)}{d}$ for every $j, 0 \leqslant j \leqslant n-1$.

Proof: By Lemma 1 and Corollary 1.

Lemma 3: Let p, q, ℓ be distinct odd primes, such that $gcd(\phi(p), \phi(q)) = d$ and ℓ is a primitive root mod p as well as a primitive root mod q. Then there exists an integer $a,\ 1 < a < pq,\ gcd(a, pq) = 1$ such that a is primitive root mod p and order of a is $\frac{\phi(q)}{d}$ mod q.

Proof: Consider the complete residue systems $S_p = \{0, 1, \ldots, p-1\}$, $S_q = \{0, 1, \ldots, q-1\}$ and $S_{pq} = \{0, 1, 2, \ldots, pq-1\}$ mod p, mod q and mod pq respectively. We define the Cartesian Product $S_p \times S_q = \{(r, s);\ r \in S_p,\ s \in S_q\}$ and a map $\theta : S_{pq} \to S_p \times S_q$ given by $\theta(a) = (r, s)$ where a ≡ r (mod p) and a ≡ s (mod q). It is easy to see that the arithmetic has a reverse (since θ is bijective) Alto retains arithmetic. Since $gcd(p, q) = 1$, ∃ integers u, v such that $pu + qv = 1$.

Given an ordered pair $(r, s) \in S_p \times S_q$, there exists a unique $a \in S_{pq}$ such that $a \equiv (spu + rqv)$ (mod pq). Then $\theta(a) = (r, s)$.

Let us now find an integer a such that $1 < a < pq$ and a is a primitive root modulo p and order of a is $\frac{\phi(q)}{d}$ modulo q, where $d = gcd(\phi(p), \phi(q))$. Now ℓ is both a primitive root mod p and an early root mod q. Choose m1 such that ℓ^{m_1} is also an early root mod p. Indeed choose m1 satisfying $1 \leqslant m_1 < \phi(p)$ and $gcd(m_1, \phi(p)) = 1$. Choose m2 such that ℓ^{dm_2} has order $\frac{\phi(q)}{d}$ mod q. Indeed choose m2 satisfying $1 \leqslant m_2 < \phi(q)$ and $gcd(dm_2, \phi(q)) = d$. Let $a \in S_{pq}$ be such that $a \equiv (\ell^{m_1} qv + \ell^{dm_2} pu)$ (mod pq). Then, $a \equiv \ell^{m_1}$ (mod p) and hence a is a primitive root mod p. Also $a \equiv \ell^{dm_2}$ (mod q) so that order of a is $\frac{\phi(q)}{d}$ mod q. Clearly, $gcd(a, pq) = 1$.

Remark 1: (i) We can also find an integer in the above lemma, by modifying p and q$a,\ 1 < a < pq$ such that $gcd(a, pq) = 1$ and a is primitive root mod q and order of a is $\frac{\phi(p)}{d}$ mod p where $d = gcd(\phi(p), \phi(q))$.

(ii) $m_1 = m_2 = 1,\ a \equiv \ell qv + \ell^d pu$ (mod pq) is one of the possible values of a.

Lemma 4: Let a bean integer with $1 < a < pq$ and $gcd(a, pq) = 1$ such that a is a primitive root mod p and order of a is $\frac{\phi(q)}{d}$ mod q OR a is a primitive root mod q and order of a is $\frac{\phi(p)}{d}$ mod p, where $d = gcd(\phi(p), \phi(q))$, then $a, a^2, a^3, \ldots, a^{d-1} \notin S$ where $S = \{1, \ell, \ell^2, \ldots, \ell^{\frac{\phi(pq)}{d} - 1}\}$.

Proof: Assume that $a^i \in S$, for some $i,\ 1 \leqslant i < d$. Then $a^i \equiv \ell^k$ (mod pq), for some $k,\ 0 \leqslant k < \frac{\phi(pq)}{d}$. However, $a \equiv \ell^{m_1} qv + \ell^{dm_2} pu$ (mod pq). Thus, $\ell^{im_1} \equiv \ell^k$ (mod p) and $\ell^{idm_2} \equiv \ell^k$ (mod q), showing that $k \equiv im_1 \pmod{\phi(p)}$ and $k \equiv idm_2 \pmod{\phi(q)}$. As d divides both φ(p) and φ(q), we obtain that $k \equiv im_1 \equiv idm_2 \equiv 0$(mod d). In particular, $im_1 \equiv 0$ (mod d), which is a contradiction as $gcd(m_1, \phi(p)) = 1$ and $1 \leqslant i < d$.

Lemma 5: There exists an integer $a,\ 1 < a < pq$ $gcd(a, pq\ell) = 1$ and $a, a^2, \ldots, a^{d-1} \notin S$, where $S = \{1, \ell, \ell^2, \ldots, \ell^{\frac{\phi(pq)}{d} - 1}\}$.

Proof: In view of Lemma 4, it is sufficient to consider $gcd(a, \ell)$. If $gcd(a, \ell) = 1$, we are through. If not, then $gcd(a, \ell) = \ell$, as ℓ is a prime. Write $a = \ell^r b$, where $\ell \nmid b$. Then b also satisfies $1 < b < pq$, $gcd(b, pq\ell) = 1$ and $b, b^2, \ldots, b^{d-1} \notin S$. For, if $b^i \in S$ for some i, $1 \leqslant i < d,\ b^i \equiv \ell^k$ (mod pq) implies that $a^i \in S$, which contradicts Lemma 4.

Lemma 6: A set integer is satisfactory $1 < a < pq,\ gcd(a, pq\ell) = 1$ and $a^i \not\equiv \ell^k$ (mod pq) for any $i, k;\ 1 \leqslant i < d$ and $0 \leqslant k < \frac{\phi(pq)}{d}$. Further, for this fixed a and any $j, 0 \leqslant j < n$, the set

$$\{1, \ell, \ldots, \ell^{\frac{\phi(p^{n-j}q)}{d}-1}, a, a\ell, \ldots, a\ell^{\frac{\phi(p^{n-j}q)}{d}-1}, \ldots, a^{d-1}, a^{d-1}\ell, \ldots$$

Proof: With a as in Lemma 5,

$$\{1, \ell, \ldots, \ell^{\frac{\phi(p^{n-j}q)}{d}-1}, a, a\ell, \ldots, a\ell^{\frac{\phi(p^{n-j}q)}{d}-1}, \ldots, a^{d-1}, a^{d-1}\ell, \ldots, a^{d-}$$

are $\phi(p^{n-j}q)$ Co-prime elements of pq. It is enough to demonstrate that both are incongruous in pairs $p^{n-j}q$. Let $a^i\ell^k \equiv a^r\ell^t \pmod{p^{n-j}q}$ with $0 \leqslant r \leqslant i < d$ and $0 \leqslant k, t < \frac{\phi(p^{n-j}q)}{d}$. Then $a^{i-r} \equiv \ell^{t-k} \pmod{p^{n-j}q}$ implies that $a^{i-r} \equiv \ell^s$ (mod pq) where $s \equiv t-k \pmod{\frac{\phi(pq)}{d}}$. Therefore, $a^{i-r} \in S$ and $0 \leqslant i-r < d$. Consequently, $i = r$. Therefore, we get $\ell^k = \ell^t \pmod{p^{n-j}q}$, where $0 \leqslant k, t < \frac{\phi(p^{n-j}q)}{d}$ and the order of ℓ mod $p^{n-j}q$ is $\frac{\phi(p^{n-j}q)}{d}$, giving us $k = t$.

SOME RESULTS

To analyze idempotents, the following results are necessary:

Lemma 9: If β is a primitive p^{k}th root of unity for an odd prime p and k a positive integer, $GF(\ell)$, then

$$\sum_{s=0}^{\phi(p^k)-1} \beta^{\ell^s} = \begin{cases} -1 & if\, k = 1, \\ 0 & if\, k \geqslant 2, \end{cases}$$

where ℓ is a primitive root mod p^k.

Proof: See Bakshi G. K. and Raka Madhu [2, Lemma 4].

Let α be a fixed primitive $p^n q$th root of unity in some extension field of $GF(\ell)$. For $0 \leqslant i \leqslant n-1$ $0 \leqslant i \leqslant n-1$, $0 \leqslant k \leqslant d-1$, define

$$A_i^{(k)} = \sum_{s \in C_{a^k}} \alpha^{p^i s}.$$

As $C_{a^k\ell} = C_{a^k}$, $(A_i^{(k)})^\ell = A_i^{(k)}$, so that each $A_i^{(k)} \in GF(\ell)$.

Lemma 10. For each $0 \leqslant i \leqslant n-1$,

$$\sum_{k=0}^{d-1} A_i^{(k)} = \begin{cases} 0 & if\, i \leqslant n-2, \\ p^{n-1} & if\, i = n-1. \end{cases}$$

Proof: For any k and i, $0 \leqslant k \leqslant d-1$, $0 \leqslant i \leqslant n-1$, $a^k p^i \ell^s \equiv a^k p^i \ell^t$ (mod pnq) if and only if $\ell^s \equiv \ell^t \pmod{p^{n-i}q}$ if and only if $s \equiv t \pmod{\frac{\phi(p^{n-i}q)}{d}}$. Therefore,

$$A_i^{(k)} = \sum_{s \in C_{a^k}} \alpha^{p^i s} = \sum_{s=0}^{\frac{\phi(p^n q)}{d}-1} \alpha^{a^k p^i \ell^s}$$

$$= \frac{\phi(p^n q)}{\phi(p^{n-i}q)} \left(\sum_{s=0}^{\frac{\phi(p^{n-i}q)}{d}-1} \alpha^{p^i a^k \ell^s} \right)$$

$$= p^i \left(\sum_{s=0}^{\frac{\phi(p^{n-i}q)}{d}-1} \beta^{a^k \ell^s} \right).$$

Where $\beta = \alpha^{p^i}$ is a primitive $p^{n-i}q$th root of unity. Therefore,

$$\{1, \ell, \ldots, \ell^{\frac{\phi(p^{n-i}q)}{d}-1}, a, a\ell, \ldots, a\ell^{\frac{\phi(p^{n-i}q)}{d}-1}, \ldots, a^{d-1}, a^{d-1}\ell, \ldots, a^{d-1}\ell^{\frac{\phi(p^{n-i}q)}{d}-1}\}$$

is a reduced residue system mod $p^{n-i}q$, the sum on the R.H.S. is

$$p^i \sum_{\substack{1 \leqslant s \leqslant p^{n-i}q \\ \gcd(s, p^{n-i}q)=1}} \beta^s = p^i \left(\sum_{t=1}^{p^{n-i}q} \beta^t - \sum_{\substack{t=1 \\ p|t}}^{p^{n-i}q} \beta^t - \sum_{\substack{t=1 \\ q|t}}^{p^{n-i}q} \beta^t + \sum_{\substack{t=1 \\ pq|t}}^{p^{n-i}q} \beta^t \right)$$

$$= p^i \left(\sum_{t=1}^{p^{n-i}q} \beta^t - \sum_{t=1}^{p^{n-i-1}q} \beta^{pt} - \sum_{t=1}^{p^{n-i}} \beta^{qt} + \sum_{t=1}^{p^{n-i-1}} \beta^{pqt} \right)$$

As $\beta \neq 1$, $\beta^p \neq 1$, $\beta^q \neq 1$, the first three geometric series are zero. If $\beta^{pq} \neq 1$, i.e. if $i \neq (n-1)$, the sum of the last series also vanishes. If $i = n-1$, the last series is $\beta^{pq} = 1$. Thus, $\sum_{k=0}^{d-1} A_i^{(k)} = p^{n-1}$ for $i = n-1$ and 0 for $i \neq n-1$.

Lemma 11: For each k, $h, 0 \leqslant k, h \leqslant d-1$ and $0 \leqslant i, j \leqslant n$,

$$\sum_{s \in C_{a^h p^j}} \alpha^{a^k p^i s} = \begin{cases} -1 & if\, i + j \geqslant n,\ j = n, \\ -\frac{\phi(p^{n-j})}{d} & if\, i + j \geqslant n,\ j \leqslant n-1, \\ \frac{1}{p^j} A_{i+j}^{(h+k)} & if\, i + j \leqslant n-1. \end{cases}$$

Proof: For $j = n$, $i + j \geqslant n$ and $C_{a^h p^j} = C_{a^h p^n} = C_{p^n}$, so that the required sum (using Lemma 9) is

$$\sum_{s \in C_{p^n}} \alpha^{a^k p^i s} = \sum_{s=0}^{\phi(q)-1} \alpha^{a^k p^{i+n} \ell^s} = \sum_{s=0}^{q-2} \beta^{\ell^s} = -1,$$

Where $\beta = \alpha^{a^{k+h} p^{i+j}}$ is a primitive qth root of unity, if $i + j \geqslant n$. Therefore, $\beta^{\ell^s} = \beta^{\ell^r}$ if and only if $\ell^s \equiv \ell^r$ (mod q), Only if s ≡ r (mod φ(q)) is accessible. The sum is then equivalent to Lemma 9.

$$\frac{\phi(p^{n-j}q)}{d \cdot \phi(q)} \left(\sum_{s=0}^{\phi(q)-1} \beta^{\ell^s} \right) = -\frac{\phi(p^{n-j})}{d}.$$

Also,

$$A_{i+j}^{(h+k)} = \sum_{s \in C_{a^{h+k}}} \alpha^{p^{i+j}s} = \sum_{s=0}^{\frac{\phi(p^nq)}{d}-1} \alpha^{p^{i+j}a^{h+k}\ell^s} = \sum_{s=0}^{\frac{\phi(p^nq)}{d}-1} \beta^{\ell^s}$$

$$= \frac{\phi(p^nq)}{d} \cdot \frac{d}{\phi(p^{n-i-j}q)} \sum_{s=0}^{\frac{\phi(p^{n-i-j}q)}{d}-1} \beta^{\ell^s} = p^{i+j} \sum_{s=0}^{\frac{\phi(p^{n-i-j}q)}{d}-1} \beta^{\ell^s}.$$

From, The lemma sum is the same $\frac{1}{p^j}A_{i+j}^{(h+k)}$. The lemma proves this.

Lemma 12: For $0 \leqslant k \leqslant d-1$, $0 \leqslant j \leqslant n-1, 0 \leqslant i \leqslant n$

$$\sum_{s \in C_{p^jq}} \alpha^{a^kp^is} = \sum_{s \in C_{p^jq}} \alpha^{p^iqs} = \begin{cases} \phi(p^{n-j}) & if\, i+j \geqslant n, \\ -p^i & if\, i+j = n-1, \\ 0 & if\, i+j \leqslant n-2. \end{cases}$$

Proof: Let r be either q or a^k for some k, $0 \leqslant k \leqslant d-1$.

The sum expected is the same as

$$p^i \sum_{s=0}^{\phi(p^{n-i-j})-1} \beta^{\ell^s} = \begin{cases} p^i \cdot 0 & \text{if}\, n-(i+j) \geqslant 2, \\ p^i \cdot (-1) & \text{if}\, n-(i+j) = 1, \end{cases}$$

$$= \begin{cases} 0 & \text{if}\, i+j \leqslant n-2, \\ -p^i & \text{if}\, i+j = n-1. \end{cases}$$

This completes the lemma proof.

Lemma 13: For $0 \leqslant i \leqslant n-1, 0 \leqslant j \leqslant n, 0 \leqslant h \leqslant d-1$,

$$\sum_{s \in C_{a^hp^j}} \alpha^{p^iqs} = \begin{cases} \phi(q) & if\, i+j \geqslant n,\ j = n, \\ \frac{\phi(p^{n-j}q)}{d} & if\, i+j \geqslant n,\ j \leqslant n-1, \\ \frac{-p^i(q-1)}{d} & if\, i+j = n-1, \\ 0 & if\, i+j \leqslant n-2. \end{cases}$$

Proof: For $j = n$, as $C_{a^hp^j} = C_{p^n}$, the required sum is $\sum_{s \in C_{p^n}} \alpha^{p^iqs} = \sum_{s=0}^{\phi(q)-1} \beta^{\ell^s} = \phi(q)$, where $\beta = \alpha^{p^{i+n}q} = 1$. For $j \leqslant n-1$ the sum is

$$\sum_{s \in C_{a^hp^j}} \alpha^{p^iqs} = \sum_{s=0}^{\frac{\phi(p^{n-j}q)}{d}-1} \beta^{\ell^s} = \frac{\phi(p^{n-j}q)}{d \cdot \phi(p^{n-j})} \sum_{s=0}^{\phi(p^{n-j})-1} \beta^{\ell^s} = \frac{\phi(q)}{d} \sum_{s=0}^{\phi(p^{n-j})-1} \beta^{\ell^s}.$$

Where $\beta = \alpha^{p^{i+j}q}$ is a primitive p^{n-i-j}th root of unity for $i+j \leqslant n-1$ and if $i+j \geqslant n$ then β = 1. Therefore, the sum is the same $\frac{\phi(q)\phi(p^{n-j})}{d}$, if i + j n. If $i+j \leqslant n-1$, The sum becomes then by Lemma 9

$$\frac{\phi(q)p^i}{d} \sum_{s=0}^{\phi(p^{n-i-j})-1} \beta^{\ell^s} = \begin{cases} 0 & \text{if}\, i+j \leqslant n-2, \\ -\frac{\phi(q)p^i}{d} & \text{if}\, i+j = n-1, \end{cases}$$

The lemma proves this

REFERENCES

[1] S.K. Arora & M. Pruthi (1999). Minimal cyclic codes of length 2pn, Finite Fields Appl. 5, pp. 177–187.

[2] G.K. Bakshi & Madhu Raka (2003). Minimal cyclic codes of length pnq, Finite Fields Appl. 9, pp. pp. 432–448.

[3] F.J. MacWilliams & N.J.A. Sloane (1977). Theory of Error-Correcting Codes, North-Holland, Amsterdam, 1977.

[4] Vera Pless : Introduction to the Theory of Error-Correcting Codes, Wiley–Intersci. Ser. Discrete Math. Optim.

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

[6] M. Pruthi (2001). Cyclic codes of length 2m, Proc. Indian Acad. Sci. Math. Sci. 111, pp. 371–379.

[7] A. Sharma, G.K. Bakshi, V.C. Dumir, M. Raka (2008). Irreducible cyclic codes of length 2n, Ars Combin. 86, pp. 133–146.

[8] Ranjeet Singh, Manju Pruthi (2011). Primitive idempotents of irreducible quadratic residue cyclic codes of length pnqm, Int. J. Algebra 5, pp. 285–294.

[9] S.K. Arora and M. Pruthi (1999). "Minimal Cyclic Codes Length 2pn ," Finite Field and their Applications, 5, pp. 177-187.

[10] Vera Pless (1988). "Introduction to the Theory of Error-Correcting Codes", WileyIntersci. Ser. Discrete Math. Optim.,

Corresponding Author

Manjeet Singh[1]* Dr. Pradeep Goel[2]

Research Scholar, Department of Mathematics, Sai Nath University, Ranchi, Jharkhand