International Journal of Research in Science And Technology http://www.ijrst.com
(IJRST) 2012, Vol. No. 2, Issue No. II, Apr-Jun **ISSN: 2249-0604**

RELATION OF ALGEBRA IN MATHEMATICAL EQUATION

Gopal Krishan Bansal
Research Scholar, Dept of Mathematics, CMJ University, Shillong

ABSTRACT

Besides the generating polynomial, there are many other polynomials that can be used to generate a cyclic code. One such another vary specific polynomial called an idempotent generator, can also be used to generate a cyclic code. As the ring R_n is semi-simple therefore each ideal in R_n contains a unique idempotent which also generates the ideal. This idempotent is called the generating idempotent of the corresponding cyclic code. The idempotent generating the minimal ideal (minimal code) in R_n *is called a* ***Primitive idempotent.***

Keywords:- polynomial, repeated roots, cyclotomic, p^nqare

INTRODUCTION

THE GROUP ALGEBRA

Definition. Let G be a multiplicative group and F be a field. Let FG denotes the set of all formal sums

$$\alpha = \sum_{g\in G, \alpha(g)\in F} \alpha(g)g$$

where $\{g\in G / \alpha(g) \neq 0\}$ is a finite set.

Then FG is a ring (associative) with respect to addition and multiplication defined as follows:

$$\sum_{g\in G} \alpha(g)g + \sum_{g\in G} \beta(g)g = \sum_{g\in G} (\alpha(g) + \beta(g))g$$

and

$$\left(\sum_{g\in G} \alpha(g)g\right)\left(\sum_{h\in G} \beta(h)h\right) = \sum_{g,h\in G} \alpha(g)\beta(h)gh$$

$$= \sum_{z\in G} \gamma(z)z$$

where $\gamma(z) = \sum_{gh=z} \alpha(g)\beta(h)$ and the sum is taken over all pairs $(g, h)\in G\times G$ such that gh=z. This ring is called the group ring of the group G over the field F.

With the scalar multiplication defined as:

$$\delta\left(\sum_{g\in G}\alpha(g)g\right) = \sum_{g\in G}(\delta\alpha(g))g$$

$$= \sum_{g\in G}\alpha(g)\,(\delta g) \text{ for all } \delta \in F,$$

FG becomes F-algebra with basis $\{g/g \in G\}$.

Definition. The ring epimorphism w: FG $\rightarrow$F defined by

$$w(\sum_{g\in G}\alpha(g)g) = \sum_{g\in G}\alpha(g)$$

is called augmentation mapping.

Remark. Let G= <g> = C_n be a cyclic group of finite order n and F be a field. Let F[x] be the ring of polynomials in indeterminate x. Then the natural homomorphism

F[x]$\rightarrow$ FG

defined by x$\rightarrow$ g is an epimorphism with kernel $<x^n-1>$, the ideal generated by x^n-1, in F[x].

Hence $FC_n \cong \dfrac{F(x)}{<x^n-1>}$.

SEMI SIMPLE GROUP ALGEBRA

Definition. The Jacobson Radical of a ring R is defined to be the intersection of all maximal ideals of R. We denote it by J(R).

Definition. A ring R is called semi simple if J(R) =0.

Definition. An element e of R is called an idempotent if $e^2 = e$.

Definition. An element e of R is called a primitive idempotent if it can not be written as sum of two orthogonal (non zero) idempotents**.**

Definition. A ring R is called Artinian if every decreasing sequence of left ideals of R is finite.

Theorem [103, p.52]. If R is semi-simple Artinian ring and M≠0 is an ideal of R, then M= eR for some idempotent e of R (the idempotent e is called generating idempotent of M).

Theorem (Wedderburn) [103, p.53]. A semi simple Artinian ring is direct sum of finite number of simple Artinian rings.

Thus in particular every semi simple Artinian ring can be written as a direct sum of finite number of minimal ideals. The generating idempotent of a minimal ideal is a **Primitive Idempotent.**

Theorem (Maschke) [103, p.143]. If F is a field, then FG is a semi simple ring if and only if G is finite and the characteristic of F does not divides the order of the group G.

QUADRATIC RESIDUES

Definition (Euler's ϕ function). For each positive integer m, the number of integers in the set {1, 2,..,m} which are relatively prime to m, denoted by $\phi(m)$, is called Euler's ϕ function. $\phi(m)$ is always even integer for all integers m >2.

If p is a prime number then for every interger $r \geq 1$,

$$\phi(p^r) = p^r - p^{r-1} = p^{r-1}(p-1).$$

It is clear that ϕ value for an odd prime is always even. In fact $\phi(m)$ is always even integer for all integers m > 2.

If m = $p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$, p_i are distinct primes and $\alpha_i \geq 0$,then

$$\phi(m) = \phi(p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r})$$

$$= \phi(p_1^{\alpha_1})\phi(p_2^{\alpha_2})\ldots\phi(p_r^{\alpha_r})$$

$$= p_1^{\alpha_1 - 1}(p_1 - 1)\, p_2^{\alpha_2 - 1}(p_2 - 1)\ldots p_r^{\alpha_r - 1}(p_r - 1).$$

Theorem. (Euler's). If a and m are positive integers with gcd (a, m) =1, then

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Definition. If gcd (a, m) =1, the least positive integer r such that $a^r \equiv 1 \pmod{m}$, is called the order of a modulo m.

By Theorem 1.3.2, $1 \leq r \leq \phi(m)$. If $r = \phi(m)$ then **a** is called **Primitive Root** modulo m.

Further, if a is a primitive root mod p^n then $a^{\frac{\phi(p^n)}{2}} \equiv -1 \pmod{p^n}$.

Definition. A set of integers { $a_1, a_2, a_3, \ldots, a_{\phi(m)}$ } such that for $i \neq j$

$$a_i \not\equiv a_j \pmod{m} \text{ and } \gcd(a_i, m) = 1$$

is called reduce residue system modulo m. If a is primitive root modulo m, then the set { 1, a, a^2 ,..., $a^{\phi(m)-1}$ } is a reduced residue system modulo m.

Definition. Let p be an odd prime.The numbers $1^2, 2^2, \ldots$ reduced modulo p are called **Quadratic Residues** modulo p or simply mod p.

To find the quadratic residues mod p it is enough to consider the square of the numbers 1 to p-1,taken modulo p.Since $(p-a)^2 \equiv a^2$ mod p'so it is sufficient to consider the numbers $1^2, 2^2, \ldots, ((p-1)/2)^2$ mod p.These are distinct.The remaining (p-1)/2 numbers modulo p are called **Quadratic Non- Residues** modulo p.

In general, if m>1 is an interger and a is any integer with g.c.d (a,m)=1,then a is called quadratic residue modulo m if the congruence $\mathbf{x^2 \equiv a \pmod{m}}$ has a solution.Otherwise a is called quadratic non residues mod m.

Theorem [86, p.76]. An integer m >1 have a primitive root if and only if m is one of the following:

2, 4, p^t, $2p^t$ where p is an odd prime and t≥1 is an arbitrary positive integer.

Theorem[93,p.95].

(a) Let p be an odd prime.Then -1 is quadratic residue modulo p iff $p \equiv 1 \pmod 4$.

(b) Product of two quadratic residues or quadratic non residues is a quadratic residue but the product of a quadratic residue and a quadratic non residue is a quadratic non residue.

CODES OVER FINITE FIELDS

We denote by $GF(p^m)$, the finite field containing p^m elements**.**

Definition. A polynomial m(x) is said to be a minimal polynomial of an element α in $GF(p^r)$ if m(x) is monic polynomial of smallest degree with coefficients in GF(p) that has α as a root. It is unique always.

Theorem [93,p.56]. Let m(x) be the minimal polynomial of an element α in $GF(p^r)$. Then

(i) m(x) is irreducible .

(ii) If α is a root of a polynomial f(x) with coefficients in GF(p), then m(x) divides f(x).

(iii) m(x) divides $x^{p^r} - x$.

(iv) if m(x) is primitive, then its degree is r. In any case the degree of m(x) is less than or equal to r.

Cyclotomic cosets. Consider the set {0, 1, 2, …, n-1}. Let l be the number such that gcd (l , n) =1. The operation of multiplication by l divides the integer's mod n into subsets called the l cyclotomic cosets mod n.

The cyclotomic coset containing the integer s is $\{s, sl, sl^2,\dots, sl^t\}$, where t is the smallest integer such that $s\, l^t \equiv s \pmod n$. We denote it by $\mathbf{C_s}$. Without loss of generality, if required we can assume that s is the smallest integer belonging to C_s.

Theorem [93, p.58]. $GF(p^s) \subseteq GF(p^r)$ if and only if s divides r and an element α in $GF(p^r)$ is in $GF(p^s)$ if and only if $\alpha^{p^s} = \alpha$.

IJRST

Assume that n is an integer and gcd (n, p) =1. Let m be the smallest integer such that $p^m \equiv 1$ mod n, then $GF(p^m)$ is the smallest field containing all the n^{th} root of unity. We now have following results:

Theorem [93, p.63]. Let α be a root of $x^n = 1$ in the smallest field F of characteristic p containing all the n^{th} root of unity and let m(x) be its minimal polynomial . Let β be a primitive n th root of unity in F and let $\alpha = \beta^s$. If C_s is the cyclotomic coset mod n containing s, then

$$m(x) = \prod_{i \in C_s} (x - \beta^i)$$

Inversion formula [80, p.200]. Let α be a primitive n th root of unity in the smallest field of characteristic p. Then the vector $C = (C_0, C_1, \ldots, C_{n-1})$ may be covered from

$C(x) = (C_0 + C_1 x + \ldots, C_{n-1} x^{n-1})$ by

$$C_i = \frac{1}{n} \sum_{j=0}^{n-1} C(\alpha^j)\alpha^{-ij}.$$

We now assume that F = GF(q) where q is a prime or some prime power. Let V(n, q) denotes the vector space over F of all n- tuples $(\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_n)$, $\alpha_i \in F$

Definition. An (m, n) block code (m < n) over GF(q) consists of an encoding function E:V(m, q)$\rightarrow$ V(n, q) and a decoding function D: V(n, q)$\rightarrow$ V(m, q).
Elements of the image of the function E are called <u>code words</u>, if $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ is a code word, we then write

$$\alpha = \alpha_1 \alpha_2 \ldots \alpha_n .$$

Definition. If $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ is in V(n, q) ,then the weight of α denoted by wt(α), is the number of positions i with $\alpha_i \neq 0$.

Definition. If $\alpha = (\alpha_1, \alpha_2, \ldots, \alpha_n)$ and $\beta = (\beta_1, \beta_2, \ldots, \beta_n)$ are two code words then the distance between α and β written as d(α , β) is equal to the number of positions i such that $\alpha_i \neq \beta_i$.

Definition. Any subspace C of V(n, q) is called a linear code over F of length n.
Thus if C is a linear code and α , $\beta \in$ C , then

d(α , β) = wt(α - β).

Definition. The minimum distance of a linear code C denoted by d(C) is defined as

$$d(C) = \min. \{ d(\alpha, \beta) / \alpha, \beta \in C, \alpha \neq \beta \}.$$

In view of Definition1.4.10,

$$d(C) = \min. \{ wt(\alpha) / \alpha \in C, \alpha \neq 0 \}.$$

IJRST

Definition. A linear code of length n, dimension k and minimum distance d is called an **[n, k, d]** code.

The parameter k; in the description of an [n, k, d] code is important, because k/n the rate of efficiency of the code depends on it. The parameter d is important because the error correcting and detecting capabilities of a code depends on it as given by the following results:

Theorem. A code with minimum distance d can correct [(d-1)/2] errors.(where [x] denotes the greatest integer less then or equal to x.). If d is even, then the code can detect d/2 errors and can correct [(d-1)/2] errors.

RESULTS & DISCUSSIONS

Theorem . If $\eta = p^n q^m$ $(n, m \geq 1)$ then the 2mn+2n+m +1 cyclotomic cosets modulo $p^n q^m$ are given by

(i) $C_0 = \{0\}$,

For $0 \leq j \leq m-1$,

(ii) $C_{p^n q^j} = \{p^n q^j, p^n q^j l, \ldots, p^n q^j \ell^{\phi(q^{m-j})-1}\}$

For $0 \leq i \leq n-1$,

(iii) $C_{p^i q^m} = \{p^i q^m, p^i q^m l, \ldots, p^i q^m \ell^{\frac{\phi(p^{n-i})}{2}-1}\}$,

(iv) $C_{gp^i q^m} = \{gp^i q^m, gp^i q^m l, \ldots, gp^i q^m \ell^{\frac{\phi(p^{n-i})}{2}-1}\}$,

For $0 \leq i \leq n-1$, $0 \leq j \leq m-1$

(v) $C_{p^i q^j} = \{p^i q^j, p^i q^j l, \ldots, p^i q^j \ell^{\frac{\phi(p^{n-i} q^{m-j})}{2}-1}\}$,

(vi) $C_{gp^i q^j} = \{gp^i q^j, gp^i q^j l, \ldots, gp^i q^j \ell^{\frac{\phi(p^{n-i} q^{m-j})}{2}-1}\}$,

where g is defined in Lemma 3.2.2

Proof.(i) $C_0 = \{0\}$ is trivial.

(ii) For $0 \leq j \leq m-1$, since l is primitive root mod q^{m-j}

$$\ell^{\phi(q^{m-j})} \equiv 1 \pmod{q^{m-j}}.$$

$$p^n \ell^{\phi(q^{m-j})} \equiv p^n \pmod{q^{m-j}}.$$

Thus

$$C_{p^n q^j} = \{p^n q^j, p^n q^j l, \ldots, p^n q^j \ell^{\phi(q^{m-j})-1}\}$$

is the cyclotomic coset containing $p^n q^j$.

(iii) For $0 \le j \le m-1$, since $O(\ell)_{p^{n-i}} = \dfrac{\phi(p^{n-i})}{2}$ implies

$$l^s \not\equiv l^t \pmod{p^{n-i}}, \quad \text{for} \quad 0 \le s, t \le \frac{\phi(p^{n-i})}{2} - 1.$$

We claim that

$$p^i q^m l^h \not\equiv p^i q^m l^k \pmod{p^n q^m}, \text{ for } \quad 0 \le h, k \le \frac{\phi(p^{n-i})}{2} - 1.$$

Let, if possible

$$p^i q\, l^h \equiv p^i q\, l^k \pmod{p^n q^m} \text{ ,then}$$

$$l^h \equiv l^k \pmod{p^{n-i}}, \quad \text{for} \quad 0 \le h, k \le \frac{\phi(p^{n-i})}{2} - 1,$$

which is a contradiction. So the set

$$C_{p^i q^m} = \{p^i q^m, p^i q^m l, \ldots, p^i q^m \ell^{\frac{\phi(p^{n-i})}{2}-1}\}$$

is cyclotomic coset containing $p^i q^m$.

(iv) On the similar lines we can prove the set

$$C_{g p^i q^m} = \{g p^i q^m, g p^i q^m l, \ldots, g p^i q^m \ell^{\frac{\phi(p^{n-i})}{2}-1}\},$$

is the cyclotomic coset containing $g p^i q^m$.

(v) For $0 \le i \le n-1$, $0 \le j \le m-1$, since $O(\ell)_{p^{n-i} q^{m-j}} = \dfrac{\phi(p^{n-i} q^{m-j})}{2}$,so we get $l^h \not\equiv l^k \bmod p^{n-i} q^{m-j}$, $0 \le h, k \le \dfrac{\phi(p^{n-i} q^{m-j})}{2} - 1$.

We claim that $p^i q^j l^s \not\equiv g p^i q^j l^t \bmod p^n q^m$, $0 \le s, t \le \dfrac{\phi(p^{n-i} q^{m-j})}{2} - 1$.

Let,if possible

$$p^i q^j l^h \equiv g p^i q^j l^k \pmod{p^n q^m}, \text{for} \quad 0 \le h, k, \le \frac{\phi(p^{n-i} q^{m-j})}{2} - 1.$$

therefore,

$$l^h \equiv l^k \bmod p^{n-i} q^{m-j}, \text{ for } 0 \le h, k \le \frac{\phi(p^{n-i} q^{m-j})}{2} - 1,$$

which is a contradiction.Hence, the set

IJRST

$$C_{p^i q^j} = \{p^i q^j, p^i q^j l, \ldots, p^i q^j \ell^{\frac{\phi(p^{n-i}q^{m-j})}{2}-1}\},$$

is cyclotomic coset containing $p^i q^j$.

(vi) On the same lines we can prove the set

$$C_{gp^i q^j} = \{gp^i q^j, gp^i q^j l, \ldots, gp^i q^j \ell^{\frac{\phi(p^{n-i}q^{m-j})}{2}-1}\},$$

is cyclotomic coset containing $gp^i q^j$.

We now claim that the cyclotomic cosets obtained in (i)-(vi) above are the only cyclotomic cosets modulo $p^n q^m$.

By constructions of cyclotomic cosets in (i)-(vi) it follows easily that:

$|C_0|=1$, ,

$|C_{p^n q^j}|=\phi(p^{m-j})$ $|C_{p^i q^m}|=|C_{gp^i q^m}|=\phi(p^{n-i})/2$.

$$|C_{p^i q^j}|=|C_{gp^i q^j}|=\frac{\phi(p^{n-i}q^{m-j})}{2}.$$

Then by order considerations, it follows that the sum:

$$|C_0| + \sum_{i=0}^{n-1}[|C_{p^i q^m}| + |C_{gp^i q^m}|] + \sum_{j=0}^{m-1}|C_{p^n q^j}| + \sum_{(i,j)=(0,0)}^{(n-1,m-1)}[|C_{p^i q^j}| + |C_{gp^i q^j}|]$$

$$=1+\sum_{i=0}^{n-1}\left[\frac{\phi(p^{n-i})}{2}+\frac{\phi(p^{n-i})}{2}\right]+\sum_{j=0}^{m-1}\phi(q^{m-j}) + \sum_{(i,j)=(0,0)}^{(n-1,m-1)}\left[\frac{\phi(p^{n-i}q^{m-j})}{2}+\frac{\phi(p^{n-i}q^{m-j})}{2}\right] = p^n q^m.$$

Hence C_0, $C_{p^n q^j}$, $C_{p^i q^m}$, $C_{gp^i q^m}$, $C_{p^i q^j}$, $C_{gp^i q^j}$ are all the cyclotomic cosets modulo $p^n q^m$.

Primitive idempotents in F[x]/ $< x^{p^n q^m} - 1 >$

For $0 \le s \le m-1$, let $C_s = \{ s, sl, \ldots, sl^{m_s - 1}\}$, where m_s is the least positive integer such that

$sl^{m_s} \equiv s \bmod m$.

If α is the primitive m^{th} root of unity in some extension of GF(l), then the polynomial.

$M^{(s)}(x) = \prod_{i \in C_s}(x - \alpha^i)$ is the minimal polynomial of α^s corresponding to C_s over GF(l). Let I_s be the minimal ideal in R_m generated by $\dfrac{x^m - 1}{M^s(s)}$ and $\theta_s(s)$ be the primitive idempotents of I_s.

Then we know that $\theta_s(\alpha^j) = \begin{cases} 1 & if \quad j \in C_s \\ 0 & if \quad j \notin C_s \end{cases}$

IJRST

Notation. For $0 \le i \le n-1 \quad , 0 \le j \le m-1,$

1. $A_{i,j} = \sum_{s\in C_g} \alpha^{p^i q^j s}, B_{i,j} = \sum_{s\in C_1} \alpha^{p^i q^j s}$

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

Clearly $A_{i,j}$ and $B_{i,j}$,,η_0 and η_1 belongs to $GF(l)$.

3. $\varepsilon_{i,r}^{j,k} = \sum_{s\in C_{p^j q^k}} \alpha^{-p^i q^r s}$, $\varepsilon_{g(i,r)}^{j,k} = \sum_{s\in C_{p^j q^k}} \alpha^{-gp^i q^r s}$, where α is primitive $p^n q^m th$ root of unity in some extension field of $GF(l)$.

4.$\sigma_{i,r}(x) = \sum_{s\in C_{p^i q^r}} x^s$, $\sigma_{g(i,r)}(x) = \sum_{s\in C_{gp^i q^r}} x^s$

Remark.

$A_{i,j} = \sum_{s\in C_g} \alpha^{p^i q^j s} = \sum_{s=0}^{\frac{\phi(p^n q^m)}{2}-1} \alpha^{gp^i q^j l^s}$. Now $\beta = \alpha^{p^i q^j}$ becomes $p^{n-i} q^{n-j}$ th root of unity,

therefore $\beta^{l^u} = \beta^{l^v}$ iff $l^u \equiv l^v \mod p^{n-i} q^{m-j}$ iff $u \equiv v \mod \frac{\phi(p^{n-i} q^{m-j})}{2}$.Therfore,

$$A_{i,j} = \sum_{s\in C_g} \alpha^{p^i q^j s} = \sum_{s=0}^{\frac{\phi(p^n q^m)}{2}-1} \alpha^{gp^i q^j l^s} = \frac{\phi(p^n q^m)}{\phi(p^{n-i} q^{m-j})} \sum_{s=0}^{\frac{\phi(p^{n-i} q^{m-j})}{2}-1} \beta^{gl^s}$$

Similarly $B_{i,j} = \frac{\phi(p^n q^m)}{\phi(p^{n-i} q^{m-j})} \sum_{s=0}^{\frac{\phi(p^{n-i} q^{m-j})}{2}-1} \beta^{l^s}.$

Proof. $\sum_{s\in C_{p^j q^k}} \alpha^{p^i q^r s} = \sum_{s=0}^{\frac{\phi(p^{n-j} q^{m-k})}{2}-1} \beta^{l^s}$ for $\beta = \alpha^{p^{i+j} q^{r+k}}$, then β is primitive $p^{n-i-j} q^{m-r-k}$ th root of unity, therefore $\beta^{l^u} = \beta^{l^v}$ $iff\ l^u \equiv l^v \mod p^{n-i-j} q^{m-r-k}$

$$iff\ u \equiv v \mod \frac{\phi(p^{n-i-j} q^{m-r-k})}{2}$$

IJRST

$$\sum_{s=0}^{\frac{\phi(p^{n-j}q^{m-k})}{2}} \beta^{l^s} = \frac{\phi(p^{n-j}q^{m-k})}{\phi(p^{n-i-j}q^{n-r-k})} \sum_{s=0}^{\frac{\phi(p^{n-i-j}q^{m-r-k})}{2}-1} \beta^{l^s}$$

Case 1: Using remark 3.3.3 ,then the above sum equals

$$\left\{ \frac{1}{p^j q^k} B_{i+j,r+k} \quad for\ (i+j) \le n-1,\ (r+k) \le m-1 \right\}$$

Case 2: when $(i+j) \ge n,\ (r+k) \le m-1$,then β is primitive q^{m-r-k} th root of unity and $\{1, l^1, l^2, .. l^{\phi(q^{n-r-k})-1}\}$ forms reduced residue system mod q^{m-r-k}, therefore ,by lemma 2.3.1,the sum is

$$\frac{\frac{\phi(p^{n-j}q^{m-k})}{2}}{\phi(q^{m-r-k})} \sum_{s=0}^{\phi(q^{m-r-k})-1} \beta^{l^s} = \begin{cases} \frac{-\phi(p^{n-j})q^{m-k-1}}{2} & if \quad r+k=m-1 \\ 0 & if \quad r+k<m-1 \end{cases}$$

Case 3: when $(i+j) \le n-1, (r+k) \ge m$, β is primitive p^{n-i-j} th root of unity and therefore by lemma 2.3.7,

$$\sum_{s \in C_{p^j q^k}} \alpha^{p^i q^r s} = \frac{\phi(p^{n-j}q^{m-k})}{\phi\, p^{n-i-j}} \sum_{s=0}^{\frac{\phi(p^{n-i-j})}{2}-1} \beta^{l^s} = \begin{cases} p^{n-j-1}\phi(q^{m-k})\eta_0 & if \quad i+j=n-1 \\ 0 & if \quad i+j<n-1 \end{cases}$$

Case 4 :when $(i+j) \ge n, (r+k) \ge n$, then $\beta = 1$,therefore the sum is $\dfrac{\phi(p^{n-j}q^{m-k})}{2}$.

REFERENCES

1. Arora, S.K and M. Pruthi, **Minimal cyclic codes of length 2p^n**, Finite Fields and their Applications 5, 177-187 (1999).

2. Arora ,S.K., Batra,S., Cohen,S.D.**Primitive idempotents of a Cyclic Group Algebra,II** , Southeast Asian Bulletin of Mathematics, (2005) 29,197-208.

3. Apostol, Tom M.**Introduction to Analytic Number Theory,** Springer-Verlag, NewYork, 1976.

4.Bakshi,G.K.;Raka,M. **Minimal cyclic codes of length p^{n}q**,Finite Fields and Their appl.9 no.4(2003)432-448

5. Bartow ,J. E.**A reduced upper bound on the error ability of codes,** IEEE Trans. Infor. Theory 9 (1963) 46.

6.**A upper bound on the error ability of codes**, IEEE Trans. Infor. Theory 9 (1963) 290.

IJRST

7. Bassalygo ,L. A.**New upper bounds for error correcting codes**, Problem of Information Transmission 1(4), 1965, 32-35.

8. Batra, S. and Arora ,S.K.**Minimal quadratic residue cyclic codes of length p^n (p odd prime),**The Korean Journal of Computational and Applied Mathematics 8(3), 531-547 (2001)

9. Batra S., Arora, S.K.**Minimal quadratic residue cyclic codes of length 2^n n>1)**,J.Appl.Math.& Computing Vol. 18 (2005),No. 1-2,25-43.

10. Berger ,Y., Be' ery ,Y.**The twisted squaring construction, trellis complexity, and generalized weight of BCH codes,** IEEE Trans. Infor. Theory 42 (1996), no.6, part 1, 1817 -1827.

11. Berlekamp ,E.R.**Algebraic Coding Theory**, McGraw Hill, New York, 1968.

12. Berlekamp, E.R. Justesen , **Some long cyclic linear binary codes are not so bad.** IEEE Trans. Infor. Theory, 20 (1974) 351-356.

13. Berlekamp,E.R., Mac.,F.J., **Gleason's Theorem on self duals codes,** IEEE Trans. Infor. Theory,19 Sloane,N.J.A (1973) 409-414.

14. Berlekamp,E.R; Sloane,N.J.A., **Restrictions on weight distribution of Reed Muller codes,** Infor.Control,14 (1969) 442-456.

15. Berlekamp, E.R.,Rumsey,H. **On the solutions of algebraic equations over** finite fields, Solomon,G. Infor. Control,10 (1967) 553-564.

16. Berman,S.D. **On theory of group codes ,** Cybernatics 3(1) (1967) 25-31.

17. Berman,S.D. **Semi simple Cyclic and Abelian codes** II, Cybernatics 3(3) (1967) 17-23.

18. Bhargawa ,V.K., Ngugen C.**Weight distribution of some cyclic codes of MacWilliams,** Second International Conference on Information Sciences and System(Univ.Patras, Patras, 1979), VolI p.p. 117-122, Reidal Dordrecht,1980.

19.Bhargava,V.K.,Stien,M. **($\upsilon,\kappa,\ \lambda$)configurations and self dual codes,** Infor. control,28 (1975) 352-355.

20. Blare, Ian F. **Distance properties of the Group code ofr Gaussian Channel**, SIAM J. Appl. Math**.** 23 (1972), 312-324.

21. Blare ,Ian F. **Permutation codes for discrete channel**, IEEE trans. Infor. Theory. 20 (1974) 138-140.

22. Blake I.F., Mullin, R.C. **The Mathematical Theory of Coding,** Acdemic press, New York,1975.