International Journal of Mathematics Trends and Technology
ISSN: 2231-5373/ https://doi.org/10.14445/22315373/IJMTT-V72I8P102

Volume 72 Issue 8, 8-10, August 2026
© 2026 Seventh Sense Research Group®

Original Article

Cyclotomic Cosets of Primitive Idempotents in Semi Simple Ring $R_{16p^nq^m} = GF(l)[x]/(x^{16p^nq^m} - 1)$

Ranjeet Singh

Department of Mathematics, Govt. College Siwani, Bhiwani, Haryana, India.

Corresponding Author : bharranjeet@yahoo.com

Received: 20 June 2026 Revised: 23 July 2026 Accepted: 13 August 2026 Published: 29 August 2026

Abstract - *We consider the ring $R_{16p^nq^m} = GF(l)[x]/(x^{16p^nq^m} - 1)$ where p, q, l are distinct odd primes, l is a primitive root, both modulo p^n and q^m such that $gcd(\varphi(p^n), \varphi(q^m))= d$ .Explicit expressions for all the 16($m \times n \times d + m + n + 1$) Cyclotomic Coset are obtained, p does not divide $q-1$ and l is of the form 16k+1.*

Keywords **-** *Cyclotomic Coset, Cyclic Codes, Minimal Cyclic Codes, Primitive Idempotent.*

MSC *: Primary 61T30; Secondary 94 B25, 11T 74.*

1. Introduction

Let GF (l) be a field of odd prime order l. Let $z \geq 1$be an integer with $gcd(l, z) = 1$.Let$R_z = \frac{GF(l)[x]}{x^z - 1}$. The minimal cyclic codes of length z over $GF(l)$ are ideals of the ring R_z. For $z = p^n$ Anuradha Sharma, G.K.Bakshi, V.C. Dumir, M. Raka, [3] obtained nd+1 "Cyclotomic Numbers and corresponding Primitive idempotents in R_zG.K. Bakshi and Madhu Raka [4] obtained $3n + 2$ primitive idempotents in $R_z$for $z = p^n q$ where p, q, l are distinct odd primes, l is a primitive root both modulo p^n and q and $gcd(\varphi(p^n), \varphi(q)) = 2$. Amita Sahni and P.T. Sehgal [5] extended the results of G.K. Bakshi and Madhu Raka and obtained $(d + 1)n + 2$ primitive idempotents in $R_z$for $z = p^n q$ where p, q, l are distinct odd primes, l is a primitive root both modulo p^n and q and $gcd(\varphi(p^n), \varphi(q)) = d$. When $d = 2$ In [5], they obtain all the results of [4]. So [4] becomes a special case of [5]. In this paper, we consider the case when Z=16 $p^n q^m$ where p, q, l are distinct odd primes, l is a primitive root both modulo p^n and q^m.Explicit expressions for all the 16($m \times n \times d + m + n + 1$) Cyclotomic Coset are obtained. $gcd(\varphi(p^n), \varphi(q^m)) = d, p$ does not divide q -1 .

Remark 2.1. For $0 \leq s \leq z - 1$, let$C_s = \{s, sl, sl^2, \ldots, sl^{t_s - 1}\}$, where t_s is the least positive integer such that $sl^{t_s} \equiv s$ (mod $16p^n q^m$) be the cyclomic coset containing s.

Lemma 2.1. Let p, q, l be distinct odd primes, n $\geq$ 1 an integer,$o(l)_{16p^{n-j}} = \varphi(16p^{n-j})$, $o(l)_{q^{m-k}} = \varphi(q^{m-k})$ and $gcd(\varphi(16p^{n-j}), \varphi(q^{m-k})) = d$ then$o(l)_{16p^{n-j}q^{m-k}} = \frac{\varphi(16p^{n-j}q^{m-k})}{d}$, for all $0 \leq j \leq n - 1$ and $0 \leq k \leq m - 1$.

Proof. Let $o(l)_{16p^{n-j}q^{m-k}} = t$, $0 \leq$ j $\leq$ n $-$ 1and $0 \leq k \leq m - 1$.Then $l^t \equiv 1 \, mod \, 16p^{n-j} \, q^{m-k}$However, p and q are distinct odd primes. Hence $l^t \equiv 1 \, mod \, 16p^{n-j}$and $l^t \equiv 1 \, mod \, q^{m-k}$.Since $o(l)_{p^{n-j}} = \varphi(8p^{n-j})$ and, $o(l)_{q^{m-k}} = \varphi(q^{m-k})$ therefore, $\varphi(16p^{n-j})$ and $\varphi(q^{m-k})$ divides t. Then, $lcm(\varphi(16p^{n-j}), \varphi(q^{m-k})) = \frac{\varphi(16p^{n-j}q^{m-k})}{d}$ divides t.On the other hand, since $o(l)_{q^{m-k}} = \varphi(q^{m-k})$, therefore, $l^{\varphi(q^{m-k})} \equiv 1 \, mod \, q^{m-k}$ hence $l^{\varphi(\frac{16p^{n-j}q^{m-k}}{d})} \equiv 1 \, mod \, q^{m-k}$.Similarly, $l^{\varphi(\frac{16p^{n-j}q^{m-k}}{d})} \equiv 1 \, mod \, p^{n-j}$. As p and q are distinct primes, we get $l^{\varphi(\frac{16p^{n-j}q^{m-k}}{d})} \equiv 1 \, mod \, 16p^{n-j} \, q^{m-k}$

Hence, $t = o(l)_{16p^{n-j}q^{m-k}}$divides $\frac{\varphi(16p^{n-j}q^{m-k})}{d}$ and we get that $t = \frac{\varphi(16p^{n-j}q^{m-k})}{d}$.

Lemma 2.2. For given p, q, ldistinct odd primes such that *g.c.d. ($\varphi(p), \varphi(q)$)=d*, and l is a primitive root mod(p) as well as q, then there always exists a fixed integer a satisfying g.c.d. (a, pq)=1,1 < a < pq, such that a is a primitive root mod(p)

and the order of a mod q is $\varphi(q)$.Also a,a^2, a^3 ,……a^{d-1} does not belong to the set S={1 , l, l^2, …, $l^{\frac{\varphi(pq)}{d}-1}$Further, for this fixed integer a and for $0 \le j \le n-1$, $0 \le k \le m-1$, the set {1 , l, l^2, …, $l^{\frac{\varphi(8p^{n-j}q^{m-k})}{d}-1}$, a, a$l$, …,a$l^{\frac{\varphi(8p^{n-j}q^{m-k})}{d}-1}$, a^2 , a$^2l$, a$^2l^2$, …, a$^2l^{\frac{\varphi(8p^{n-j}q^{m-k})}{d}-1}$a^{d-1} , a^{d-1} l, …, a^{d-1} $l^{\frac{\varphi(8p^{n-j}q^{m-k})}{d}-1}$forms a reduced residue system modulo $16p^{n-j}q^{m-k}$.

Proof: See Lemma 4 [8]

Theorem. 2.1. If $\eta = 16p^nq^m$ (m, n ≥ 1)). Then the $16(m \times n \times d + m + n + 1)$ Cyclotomic cosets modulo $16p^nq^m$are given by (i) C$_0$= {0} , $(ii)C_{p^nq^m}$= {p^nq^m },$(iii)C_{2p^nq^m}$= {$2p^nq^m$ },$(iv)C_{3p^nq^m}$= {$3p^nq^m$ },$(v)C_{4p^nq^m}$= {$4p^nq^m$ }, $(vi)C_{5p^nq^m}$= {$5p^nq^m$ },$(vii)C_{6p^nq^m}$= {$6p^nq^m$ }, $(viii)C_{7p^nq^m}$= {$7p^nq^m$ } …………$(xvi)C_{15p^nq^m}$= {$15p^nq^m$ }. For $0 \le k \le m-1$

C_{p^n}= {p^n, p^nl, …,$p^nl^{\varphi(q^{m-k})-1}$} , $(iv)C_{2p^n}$= {$2p^n$, $2p^nl$, …, $2p^nl^{\varphi(q^{m-k})-1}$} , $(v)C_{3p^n}$= {$3p^n$, $3p^nl$, …, $3p^nl^{\varphi(q^{m-k})-1}$} , , $(vi)C_{4p^n}$= {$4p^n$, $4p^nl$, …, $4p^nl^{\varphi(q^{m-k})-1}$} , , $(vii)C_{5p^n}$= {$5p^n$, $5p^nl$, …, $5p^nl^{\varphi(q^{m-k})-1}$} , , $(viii)C_{6p^n}$= {$6p^n$, $6p^nl$, …, $6p^nl^{\varphi(q^{m-k})-1}$} , , $(ix)C_{7p^n}$= {$7p^n$, $7p^nl$, …, $7p^nl^{\varphi(q^{m-k})-1}$} ……………………

, $(xv)C_{15p^n}$= {$15p^n$, $15p^nl$, …, $15p^nl^{\varphi(q^{m-k})-1}$} and for $0 \le j \le n-1$,

$(i)C_{q^m}$= {q^m, q^ml, …, $q^ml^{\varphi(p^{n-j})-1}$}

(ii)C_{2q^m}= {$2q^m$,$2q^ml$, …, $2q^ml^{\varphi(p^{n-j})-1}$Similarly, we can obtain the remaining 14 Cyclotomic cosets.

For $0 \le j \le n-1$, and $0 \le k$, $\le m-1$ for $0 \le w \le d-1$,

(i)$C_{a^wp^jq^k}$={ $a^wp^jq^k$,$a^wp^jq^kl$, …,$a^wp^jq^k$ $l^{\frac{\varphi(2p^{n-j}q^{m-k})}{d}-1}$} ,$(ii)$ $C_{2a^wp^jq^k}$={ $2a^wp^jq^k$,$2a^wp^jq^kl$, …,$2a^wp^jq^k$ $l^{\frac{\varphi(2p^{n-j}q^{m-k})}{d}-1}$} where the number a is given by Lemma 4[9] Similarly we can obtain remaining 14 Cyclotomic cosets..

Proof:-As per the construction of the above cyclotomic cosets from (i) to (Viii), we can check that these are the only cyclotomic cosets. Also, we can see that order of C$_0$= {0}, $(ii)C_{p^nq^m}$= {p^nq^m } is one, i.e., IC$_0$I=1 I$C_{p^nq^m}$I=1, for $0 \le k \le m-1$ order of l modulo q^{m-k} $\varphi(q^{m-k})$ so the cardinality of C_{p^n} and C_{2p^n} is $\varphi(q^{m-k})$. Similarly, for $0 \le j \le n-1$, so the cardinality of C_{q^m} and C_{2q^m} is $\varphi(p^{n-j}$).On Similar lines, we can see for $0 \le j \le n-1$, $0 \le k \le m-1$ and $0 \le w \le d-1$,

I$C_{a^wp^jq^k}$I $=\frac{\varphi(2p^{n-j}q^{m-k})}{d}$, I$C_{2a^wp^jq^k}$I $=\frac{\varphi(2p^{n-j}q^{m-k})}{d}$,

$$Then, by\ order\ considerations, it\ follows\ that\ the\ sum$$

$$IC_0I + IC_{p^nq^m}I + IC_{2p^nq^m}I + IC_{3p^nq^m}I + IC_{4p^nq^m}I + IC_{5p^nq^m}I + IC_{6p^nq^m}I + IC_{7p^nq^m}I + \cdots \ldots\ldots\ldots\ldots\ldots..IC_{15p^nq^m}I + IC_{p^n}\ I + IC_{2p^n}I + IC_{3p^n}\ I + IC_{4p^n}\ I + IC_{5p^n}\ I + IC_{6p^n}\ I + IC_{7p^n}\ I + \cdots \ldots\ldots\ldots\ldots\ldots\ldots IC_{15p^n}\ I + IC_{q^m}\ I + IC_{2q^m}\ I + IC_{3q^m}\ I + IC_{4q^m}\ I + IC_{5q^m}\ I + IC_{6q^m}\ I + IC_{7q^m}\ I + \cdots \ldots\ldots\ldots\ldots\ldots\ldots. IC_{15q^m}\ I +$$

$$\sum_{j=0}^{n-1}.\sum_{k=0}^{m-1}.\sum_{w=0}^{d-1}\{IC_{a^wp^jq^k}I + IC_{2a^wp^jq^k}I + IC_{3a^wp^jq^k}I + IC_{4a^wp^jq^k}I + IC_{5a^wp^jq^k}I + IC_{6a^wp^jq^k}I + IC_{7a^wp^jq^k}I + \cdots \ldots\ldots\ldots\ldots. + IC_{15a^wp^jq^k}I\ \}.$$

$$=8+8+16\sum_{k=0}^{m-1}.\varphi(q^{m-k}) + 16\sum_{j=0}^{n-1}.\varphi(p^{n-j}) + 16\sum_{j=0}^{n-1}.\sum_{k=0}^{m-1}\frac{\varphi(2p^{n-j}q^{m-k})}{d} = 16p^nq^m.$$

References

[1] Anuradha Sharma et al., "Cyclotomic Numbers and Primitive Idempotents in the Ring GF(q) [x]/(x^{p^n}1)," *Finite Fields and Their Applications*, vol. 10, no. 4, pp. 653-673, 2004. [CrossRef] [Google Scholar] [Publisher Link]

[2] Gurmeet K. Bakshi, and Madhu Raka, "Minimal Cyclic Codes of Length $p^n q$," *Finite Fields and Their Applications*, vol. 9, no. 4, pp. 432-448, 2003. [CrossRef] [Google Scholar] [Publisher Link]

[3] Amita Sahni, and Poonam Trama Sehgal, "Minimal Cyclic Codes of Length p^nq," *Finite Fields and Their Applications*, vol. 18, no. 5, pp. 1017-1036, 2012. [CrossRef] [Google Scholar] [Publisher Link]

[4] Gurmeet Kaur Bakshi, Madhu Raka, and Anuradha Sharma, "Idempotent Generators of Irreducible Cyclic Codes," *Number Theory & Discrete Geometry*, vol. 6, pp. 13-18, 2008. [Google Scholar]

[5] Ranjeet Singh, and Manju Pruthi, "Primitive Idempotents of Irreducible Quadratic Residue Cyclic Codes of Length p^nq^m," *International Journal of Algebra*, vol. 5, no. 5-8, pp. 285-294, 2011. [Google Scholar] [Publisher Link]

[6] Florence Jessie MacWilliams, and Neil James Alexander Sloane, *The Theory of Error-Correcting Codes*, vol. 16, Elsevier, 1977. [Google Scholar]

[7] Vera Pless, *Introduction to the Theory of Error-Correcting Codes*, John Wiley & Sons, 1988. [Google Scholar]

[8] George Nemhauser, and Laurence Wolsey, *Wiley-Interscience Series in Discrete Mathematics and Optimization*, Wiley, 1998. [CrossRef] [Google Scholar] [Publisher Link]

[9] Jagbir Singh, and Sonika Ahlawat, "Some Cyclic Codes of Length 4pn and Their Minimum Distance Bounds," *International Journal of Applied Engineering Research*, vol. 13, no. 23, pp. 16708-16718, 2018. [Publisher Link]

[10] Jagbir 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," *Journal of Applied Mathematics and Computing*, vol. 48, no. 1-2, pp. 55-69, 2014. [CrossRef] [Google Scholar] [Publisher Link]

[11] Jagbir Singh, S.K. Arora, and Sheetal Chawla, "Some Cyclic Codes of Length $8p^n$," *International Journal of Pure and Applied Mathematics*, vol. 116, no. 1, pp. 217-241, 2017. [CrossRef] [Google Scholar]

[12] Ranjeet Singh, "Some Cyclotomic Cosets in the Ring R_(8p^n q^m)=GF(l)[x] (x^(8p^n q^m)-1)," *International Journal of Advanced Research*, vol. 14, no. 4, pp. 93-939, 2026. [CrossRef] [Publisher Link]