

Journal Homepage: - www.journalijar.com

INTERNATIONAL JOURNAL OF ADVANCED RESEARCH (IJAR)

Article DOI: 10.21474/IJAR01/23266
DOI URL: <http://dx.doi.org/10.21474/IJAR01/23266>



RESEARCH ARTICLE

SOME CYCLOTOMIC COSETS IN THE RING $R_{8p^n q^m} = GF(l)[x]/(x^{8p^n q^m} - 1)$

Ranjeet Singh

1. Associate Professor Department of Mathematics Govt. College Siwani, (Bhiwani) (Haryana) India.

Manuscript Info

Manuscript History

Received: 10 February 2026
Final Accepted: 12 March 2026
Published: April 2026

Key words:-

Cyclotomic Coset, Cyclic Codes,
Generating Polynomials, and Minimal
Cyclic Codes.

Abstract

We consider the ring $R_{8p^n q^m} = GF(l)[x]/(x^{8p^n q^m} - 1)$ 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 $8(m \times n \times d + m + n + 1)$ Cyclotomic Coset are obtained, p does not divide $q-1$ and l is of the form $8k+1$.

"© 2026 by the Author(s). Published by IJAR under CC BY 4.0. Unrestricted use allowed with credit to the author."

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 $z = p^n$ S.K. Arora and Manju Pruthi [1] obtained $n+1$ primitive idempotents in R_z . Again for $z = 2p^n$ S.K. Arora and Manju Pruthi [2] obtained $2n + 2$ primitive idempotents in 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_z ". G.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 $Z = 8p^n q^m$ 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 $8(m \times n \times d + m + n + 1)$ Cyclotomic Coset are obtained. $gcd(\varphi(p^n), \varphi(q^m)) = d$, p does not divide -1 . Here, we extend the results of Amita Sahni and P.T. Sehgal [5].

Remark:-

For $0 \leq s \leq z - 1$, let $C_s = \{s, sl, sl^2, \dots, sl^{t_s-1}\}$, where t_s is the least positive integer such that $sl^{t_s} \equiv s \pmod{8p^n q^m}$ be the cyclotomic coset containing s .

Lemma:-

Let p, q, l be distinct odd primes, $n \geq 1$ an integer, $o(l)_{8p^{n-j}} = \varphi(8p^{n-j})$, $o(l)_{q^{m-k}} = \varphi(q^{m-k})$ and $gcd(\varphi(8p^{n-j}), \varphi(q^{m-k})) = d$ then $o(l)_{8p^{n-j} q^{m-k}} = \frac{\varphi(8p^{n-j} q^{m-k})}{d}$, for all $0 \leq j \leq n - 1$ and $0 \leq k \leq m - 1$.

Corresponding Author:- Ranjeet Singh

Address:- Associate Professor Department of Mathematics Govt. College Siwani, (Bhiwani) (Haryana) India.

Proof:-

Let $o(l)_{8p^{n-j}q^{m-k}} = t, 0 \leq j \leq n-1$ and $0 \leq k \leq m-1$. Then $l^t \equiv 1 \pmod{8p^{n-j}q^{m-k}}$. But p and q are distinct odd primes. Hence $l^t \equiv 1 \pmod{8p^{n-j}}$ and $l^t \equiv 1 \pmod{q^{m-k}}$. Since $o(l)_{p^{n-j}} = \varphi(8p^{n-j})$ and $o(l)_{q^{m-k}} = \varphi(q^{m-k})$ therefore, $\varphi(8p^{n-j})$ and $\varphi(q^{m-k})$ divides t . Then, $lcm(\varphi(8p^{n-j}), \varphi(q^{m-k})) = \frac{\varphi(8p^{n-j}q^{m-k})}{d}$ divides t . On the other hand, since $o(l)_{q^{m-k}} = \varphi(q^{m-k})$, therefore, $l^{\varphi(q^{m-k})} \equiv 1 \pmod{q^{m-k}}$ hence $l^{\varphi(\frac{8p^{n-j}q^{m-k}}{d})} \equiv 1 \pmod{q^{m-k}}$. Similarly, $l^{\varphi(\frac{8p^{n-j}q^{m-k}}{d})} \equiv 1 \pmod{p^{n-j}}$. As p and q are distinct primes, therefore, we get $l^{\varphi(\frac{2p^{n-j}q^{m-k}}{d})} \equiv 1 \pmod{8p^{n-j}q^{m-k}}$. Hence, $t = o(l)_{8p^{n-j}q^{m-k}}$ divides $\frac{\varphi(8p^{n-j}q^{m-k})}{d}$ and we get that $t = \frac{\varphi(8p^{n-j}q^{m-k})}{d}$.

Lemma:-

For given p, q, l distinct 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 $a, a^2, a^3, \dots, a^{d-1}$ does not belong to the set $S = \{1, l, l^2, \dots, l^{\frac{\varphi(pq)}{d}-1}\}$. Further, for this fixed integer a and for $0 \leq j \leq n-1, 0 \leq k \leq m-1$ the set $\{1, l, l^2, \dots, l^{\frac{\varphi(8p^{n-j}q^{m-k})}{d}-1}, a, al, \dots, al^{\frac{\varphi(8p^{n-j}q^{m-k})}{d}-1}, a^2, a^2l, a^2l^2, \dots, a^2l^{\frac{\varphi(8p^{n-j}q^{m-k})}{d}-1} a^{d-1}, a^{d-1}l, \dots, a^{d-1}l^{\frac{\varphi(8p^{n-j}q^{m-k})}{d}-1}\}$ forms a reduced residue system modulo $8p^{n-j}q^{m-k}$.

Proof: Similar Lemma 4 [10]

Theorem:-

If $\eta = 8p^n q^m$ ($m, n \geq 1$), Then the $8(m \times n \times d + m + n + 1)$ Cyclotomic cosets modulo $8p^n q^m$ are given by (i) $C_0 = \{0\}$, (ii) $C_{p^n q^m} = \{p^n q^m\}$, (iii) $C_{2p^n q^m} = \{2p^n q^m\}$, (iv) $C_{3p^n q^m} = \{3p^n q^m\}$, (v) $C_{4p^n q^m} = \{4p^n q^m\}$, (vi) $C_{5p^n q^m} = \{5p^n q^m\}$, (vii) $C_{6p^n q^m} = \{6p^n q^m\}$, (viii) $C_{7p^n q^m} = \{7p^n q^m\}$. For $0 \leq k \leq m-1$
 $C_{p^n} = \{p^n, p^n 1, \dots, p^n l^{\varphi(q^{m-k})-1}\}$, (iv) $C_{2p^n} = \{2p^n, 2p^n 1, \dots, 2p^n l^{\varphi(q^{m-k})-1}\}$, (v) $C_{3p^n} = \{3p^n, 3p^n 1, \dots, 3p^n l^{\varphi(q^{m-k})-1}\}$, (vi) $C_{4p^n} = \{4p^n, 4p^n 1, \dots, 4p^n l^{\varphi(q^{m-k})-1}\}$, (vii) $C_{5p^n} = \{5p^n, 5p^n 1, \dots, 5p^n l^{\varphi(q^{m-k})-1}\}$, (viii) $C_{6p^n} = \{6p^n, 6p^n 1, \dots, 6p^n l^{\varphi(q^{m-k})-1}\}$, (ix) $C_{7p^n} = \{7p^n, 7p^n 1, \dots, 7p^n l^{\varphi(q^{m-k})-1}\}$ and for $0 \leq j \leq n-1$,

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

(ii) $C_{2q^m} = \{2q^m, 2q^m 1, \dots, 2q^m l^{\varphi(p^{n-j})-1}\}$ Similarly we can obtain remaining 6 Cyclotomic cosets.

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

(i) $C_{a^w p^j q^k} = \{a^w p^j q^k, a^w p^j q^k 1, \dots, a^w p^j q^k l^{\frac{\varphi(2p^{n-j}q^{m-k})}{d}-1}\}$, (ii) $C_{2a^w p^j q^k} = \{2a^w p^j q^k, 2a^w p^j q^k 1, \dots, 2a^w p^j q^k l^{\frac{\varphi(2p^{n-j}q^{m-k})}{d}-1}\}$ where the number a is given by Lemma 4[10] Similarly we can obtain remaining 6 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) $C_{p^n q^m} = \{p^n q^m\}$ is one, i.e., $IC_0 = 1$ $IC_{p^n q^m} = 1$, for $0 \leq k \leq m-1$ 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 $0 \leq j \leq n-1$, so the cardinality of C_{q^m} and C_{2q^m} is $\varphi(p^{n-j})$. On Similar lines, we can see For $0 \leq j \leq n-1, 0 \leq k \leq m-1$ and $0 \leq w \leq d-1$,

$$IC_{a^w p^j q^k} = \frac{\varphi(2p^{n-j}q^{m-k})}{d}, IC_{2a^w p^j q^k} = \frac{\varphi(2p^{n-j}q^{m-k})}{d},$$

Then, by order considerations, it follows that the sum

$$IC_0I + IC_{p^n q^m} I + IC_{2p^n q^m} I + IC_{3p^n q^m} I + IC_{4p^n q^m} I + IC_{5p^n q^m} I + IC_{6p^n q^m} I + IC_{7p^n q^m} I + IC_{p^n} I + IC_{2p^n} I + IC_{3p^n} I + IC_{4p^n} I + IC_{5p^n} I + IC_{6p^n} I + IC_{7p^n} I + IC_{q^m} I + IC_{2q^m} I + IC_{3q^m} I + IC_{4q^m} I + IC_{5q^m} I + IC_{6q^m} I + IC_{7q^m} I +$$

$$\sum_{j=0}^{n-1} \cdot \sum_{k=0}^{m-1} \cdot \sum_{w=0}^{d-1} \{IC_{a^w p^j q^k} I + IC_{2a^w p^j q^k} I + IC_{3a^w p^j q^k} I + IC_{4a^w p^j q^k} I + IC_{5a^w p^j q^k} I + IC_{6a^w p^j q^k} I + IC_{7a^w p^j q^k} I\}.$$

$$=4+4+8 \sum_{k=0}^{m-1} \cdot \varphi(q^{m-k}) + 8 \sum_{j=0}^{n-1} \cdot \varphi(p^{n-j}) + 8 \sum_{j=0}^{n-1} \cdot \sum_{k=0}^{m-1} \frac{\varphi(2p^{n-j} q^{m-k})}{d} = 8p^n q^m.$$

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) $[x]/\langle x^{p^n} - I \rangle$ ”, Finite Fields Appl. 10 (2004) 653-673.
 [4] G.K.Bakshi, Madhu Raka, “Minimal cyclic codes of length $p^n q^n$ ”, Finite Fields Appl. 9 (2003) 432-448.
 [5] A.Sahni and P.T.Sehgal, “Minimal Cyclic Codes of length $p^n q^n$,” Finite Fields Appl. 18 (2012) 1017-1036.
 [6] G.K.Bakshi, Madhu Raka, “Idempotent Generators of Irreducible Cyclic Codes” Ramanujan Math Soc, Mysore (2008) 13-18.
 [7] Ranjeet Singh, M.Pruthi, “Primitive Idempotents of Irreducible Quadratic Residue Cyclic Codes of Length $p^n q^m$ ” International Journal of Algebra vol.5 (2011) 285-294.
 [8] F.J. Mac Williams & N.J.A. Sloane; The Theory of Error-Correcting Codes, Bell Laboratories, Murray Hill NJ 07974 U.S.A.
 [9] Vera Pless, “Introduction to the Theory of Error-Correcting Codes”, Wiley-Intersci. Ser. Discrete Math. Optim., (1998).
 [10] A.Sahni and P.T.Sehgal, “Minimal Cyclic Codes of length $p^n q^n$,” Finite Fields Appl. 18 (2012) 1017-1036.
 [11] J. Singh, S. Ahlawat, Some cyclic codes of length $4p^n$ and their minimum distance bounds, Int. J. Appl. Eng. Res. 13 (2018), 16708-16718.
 [12] J. Singh, 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), 55-69.
 [13] J. Singh, S.K. Arora, S. Chawla, Some cyclic codes of length $8p^n$, Int. J. Pure Appl. Math. 116 (2017), 217-241.