International Journal of Mathematics Trends and Technology
ISSN: 2231 – 5373 / https://doi.org/10.14445/22315373/IJMTT-V68I4P513

Volume 68 Issue 4, 84-86, April 2022

Original Article

Cyclotomic Cosets in the Ring $R_{2p^nq} = GF(l)[x]/(x^{2p^nq} - 1)$ (n ≥ 1)

Ranjeet Singh

Department of Mathematics Govt. College Siwani (Bhiwani) (Haryana) India.

Received Date: 17 March 2022
Revised Date: 19 April 2022
Accepted Date: 30 April 2022

Abstract - *Explicit expressions for all the 2n(d+1)+4* Cyclotomic Cosets *in the ring* $R_{2p^nq} = GF(l)[x]/(x^{2p^nq} - 1)$, *where p, q, l are distinct odd primes* $o(l)_{2p^n} = \phi(2p^n)$, *(n ≥ 1) and* $o(l)_q = \phi(q)$ *with gcd (*$\phi(2p^n)$, $\phi(q)$*)=d, are obtained.*
Keywords - *Primitive root, Cyclotomic coset.*

2000 AMS Mathematical Subject Classification: *20C05, 94B05, 16S34.*

I. INTRODUCTION

Let GF(l) be a field of odd prime order l. Let $m \geq 1$ be an integer with gcd(l,m)=1. Let $R_m = GF(l)[x]/(x^m - 1)$. In this paper, we consider the case when $m = 2p^nq$ where p, q and l are distinct odd primes and $o(l)_{2p^n} = \phi(2p^n)$, (n ≥ 1) and $o(l)_q = \phi(q)$ with gcd ($\phi(2p^n)$, $\phi(q)$)=d. We obtain explicit expressions for all the *2(d+1)n+4* Cyclotomic coset in R_{2p^nq} (see theorem2.3).

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

LEMMA 2.1 Let p, q, l be distinct odd primes, n ≥ 1 an integer, $o(l)_{2p^{n-j}} = \phi(2p^{n-j})$, $o(l)_q = \phi(q)$ and gcd $(\phi(2p^{n-j}), \phi(q))$ =d, then $o(l)_{2p^{n-j}q} = \frac{\phi(2p^{n-j}q)}{d}$, for all j, 0 ≤ j ≤ n – 1.

Proof. Let $o(l)_{2p^{n-j}q} = \lambda_j$, 0 ≤ j ≤ n – 1. Then, $l^{\lambda_j} \equiv 1$ (mod $2p^{n-j}q$), but p and q are distinct odd primes. Hence $l^{\lambda_j} \equiv 1$(mod $2p^{n-j}$) and $l^{\lambda_j} \equiv 1$(mod q). Since $o(l)_{2p^{n-j}} = \phi(2p^{n-j})$ and, $o(l)_q = \phi(q)$ therefore, $\phi(2p^{n-j})$ and $\phi(q)$ divides λ_j. Then lcm($\phi(2p^{n-j})$, $\phi(q)$)= $\frac{\phi(2p^{n-j}q)}{d}$ divides λ_j. On the other hand, since $o(l)_q = \phi(q)$, therefore, $l^{\phi(q)} \equiv 1$ (mod q) hence $l^{\phi(\frac{2p^{n-j}q}{d})} \equiv 1$(mod q). Similarly, $o(l)_{2p^{n-j}} = \phi(2p^{n-j})$, yields $l^{\phi(\frac{2p^{n-j}q}{d})} \equiv 1$(mod p^{n-j}). As p and q are distinct primes, therefore, we get $l^{\phi(\frac{2p^{n-j}q}{d})} \equiv 1$ (mod $2p^{n-j}q$),
Hence, $\lambda_j = o(l)_{2p^{n-j}q}$ divides $\frac{\phi(2p^{n-j}q)}{d}$ and we get that $\lambda_j = \frac{\phi(2p^{n-j}q)}{d}$.

LEMMA 2.2 For given p, q, l distinct odd primes such that *gcd (*$\phi(p)$, $\phi(q)$*)=d*, and l is primitive root mod(p) as well as q then there always exists fixed integer a satisfying gcd(a, 2pq)=1, ,1 < a < 2pq, such that a is primitive root mod(p) and order of a mod q is $\frac{\phi(q)}{d}$. Also a,a^2, a^3 ,……a^{d-1} does not belong to the set S={1 , l , l^2, …, $l^{\frac{\phi(2p\ q)}{d}-1}$. Further for this fixed integer a and for 0 ≤ j ≤ n – 1, the set {1 , l , l^2, …, $l^{\frac{\phi(2p^{n-j}q)}{d}-1}$, a, a$l$, …,a$l^{\frac{\phi(2p^{n-j}q)}{d}-1}$, a^2 , $a^2 l$, $a^2 l^2$, …, $a^2 l^{\frac{\phi(2p^{n-j}q)}{4}-1}$, a^{d-1}, $a^{d-1} l$, …, $a^{d-1} l^{\frac{\phi(2p^{n-j}q)}{d}-1}$} forms a reduced residue system modulo $2p^{n-j}q$

Proof . Trivial

THEOREM 2.3 If $\eta =$ $2p^nq$ ($n \geq 1$), then the *2n(d+1)+4* cyclotomic cosets modulo $2p^nq$ are given by (i) $C_0= \{0\}$ (ii) $C_{p^nq} = \{ p^nq \}$ (iii) $C_{p^n} = \{p^n, p^nl, \ldots, p^n l^{\phi(q)-1}\}$, (iv) $C_{2p^n} = \{2p^n, 2p^nl, \ldots, 2p^n l^{\phi(q)-1}\}$ and for $0 \leq j \leq n-1$,

(v) $C_{p^jq} = \{p^jq, p^jql, \ldots, p^j q\, l^{\phi(p^{n-j})-1}\}$, (vi) $C_{2p^jq} = \{2p^jq, 2p^jql, \ldots, 2p^jq\, l^{\phi(p^{n-j})-1}\}$

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

(vii) $C_{a^kp^j} = \{a^k p^j, a^k p^jl, \ldots, a^k p^j\, l^{\frac{\phi(p^{n-j}q)}{d}-1}\}$

(viii) $C_{2a^kp^j} = \{2 a^k p^j, 2 a^k p^jl, \ldots, 2 a^k p^j\, l^{\frac{\phi(p^{n-j}q)}{d}-1}\}$ .where the number a is given by Lemma2.2.

Proof (i) $C_0 = \{0\}$, (ii) $C_{p^nq} = \{ p^nq \}$are trivial

(iii) since $o(l)_q = \phi(q)$, therefore, $l^{\phi(q)} \equiv 1 \pmod{2q}$

$p^n\, l^{\phi(q)} \equiv p^n \pmod{2 p^n q}$

.Hence $C_{p^n} = \{p^n, p^nl\ldots, p^n l^{\phi(q)}\}$ is the cyclotomic coset containing p^n.

(iv)Similarly $C_{2p^n} = \{2p^n, 2p^nl, \ldots, 2p^n l^{\phi(q)-1}\}$

is the cyclotomic coset containing $2p^n$.

(v) As by our choice for $0 \leq j \leq n-1$, $o(l)_{2p^{n-j}} = \phi(2p^{n-j})$, therefore, $l^{\phi(2p^{n-j})} \equiv 1 \pmod{2p^{n-j}}$.Let, if possible $p^j q\, l^h \equiv p^j q\, l^k \pmod{2p^n q}$,for some $h \neq k$, $0 \leq h, k \leq \phi(2p^{n-j})-1$.By dividing the above congruence by p^jq, we get $l^h \equiv l^k \pmod{2p^{n-j}}$, which is a contradiction, since by our choice $h-k < \phi(2p^{n-j})$ and $o(l)_{2p^{n-j}} = \phi(2p^{n-j})$ .Therefore, the set $C_{p^jq} = \{p^jq, p^jql , \ldots, p^jq\, l^{\phi(p^{n-j})-1}\}$is cyclotomic coset containing $p^j q$.

(vi) Similarly, $C_{2p^jq} = \{2p^jq, 2p^jql , \ldots, 2p^jq\, l^{\phi(p^{n-j})-1}\}$is cyclotomic coset containing $2p^j q$. (vii) By lemma2.1, $o(l)_{2p^{n-j}q} = \frac{\phi(2p^{n-j}q)}{d}$ .Then, for integers h, k such that $0 \leq h, k \leq \frac{\phi(2p^{n-j}q)}{d}-1$,we get that $l^h \not\equiv l^k \pmod{2p^{n-j}q}$.Since p is co prime to both l and q ,therefore it follows that for given integer j, $0 \leq j \leq n-1$,we have $p^j\, l^h \not\equiv p^j\, l^k \pmod{2p^n q}$. Also $(a,pql)=1$ So $a^k p^j\, l^h \not\equiv a^k p^j\, l^k \pmod{2p^n q}$. Thus the set $C_{a^kp^j} = \{a^k p^j, a^k p^jl, \ldots, a^k p^j\, l^{\frac{\phi(p^{n-j}q)}{d}-1}\}$ is cyclotomic coset containing $C_{a^kp^j}$. (viii) On similar lines, the set $C_{2a^kp^j} = \{2 a^k p^j, 2 a^k p^jl, \ldots, 2 a^k p^j\, l^{\frac{\phi(p^{n-j}q)}{d}-1}\}$is cyclotomic coset containing $C_{2a^kp^j}$. . We now claim that the cyclotomic cosets obtained in (i)-(viii) above are the only cyclotomic cosets modulo $2p^nq$. By constructions of cyclotomic cosets in (i)-(viii) it follows easily that: Then by order considerations, it follows that the sum:

$$|C_0| + |C_{p^nq}| + |C_{p^n}| + |C_{2p^n}|$$

$$+\sum_{k=0}^{d-1}\sum_{j=0}^{n-1} |C_{a^kp^j}| + |C_{2a^kp^j}| + \sum_{j=0}^{n-1}[|C_{p^jq}| + |C_{2p^jq}|$$

$$= 2 + |\phi(q)| + |\phi(q)| + \sum_{j=0}^{n-1}(2d\,\frac{\phi(p^{n-j}q)}{d} + 2\phi(p^{n-j})$$

$$= 2+2\phi(q)+2\sum_{j=0}^{n-1}\{\phi(p^{n-j}) + \phi(p^{n-j}q)\} = 2q + 2q\sum_{j=0}^{n-1}\phi(p^{n-j}) = 2q + 2q(p^n-1) = 2p^nq.$$

II. CONCLUSION

As the code of length 2k + 1 is capable of detecting 2k errors and correcting k errors. So the following conclusions are made for error correction and detection capabilities of the cyclic codes when *2n(d+1)+4* the cyclotomic cosets are obtained in the ring $R_{2p^nq} = GF(l)[x]/(x^{2p^nq} - 1)$ the corresponding primitive idempotents are also obtained and consequently the minimum distance of the cyclic codes may be obtained which help in the correction and detection of transmission errors.

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^nq, Finite Fields Appl. 9 (2003) 432-448.

[5] G.K.Bakshi, Madhu Raka, Idempotent Generators of Irreducible Cyclic Codes, Ramanujan Math Soc, Mysor. (2008) 13-18.

[6] Ranjeet Singh, M.Pruthi, Primitive Idempotents of Irreducible Quadratic Residue Cyclic Codes of Length p^nq^m, International Journal of Algebra. 5 (2011) 285-294.

[7] Ian F. Blare, Permutation Codes For Discrete Channel, IEEE Trans. Inform. Theory. 20 (1974) 138-140.

[8] Ivan Niven and Herbert S. Zuckerman, An Introduction to the Theory of Numbers, John Wiley and Sons Inc, New York. (1960).

[9] J. E. Bartow, A Reduced Upper Bound on the Error Ability of Codes, IEEE Trans. Inform. Theory. 9 (1963) 46.

[10] J. E. Bartow, A upper Bound on the Error Ability of Codes, IEEE Trans. Inform. Theory. 9 (1963) 290.

[11] J. H. Conway and N. J. A. Sloane, Self Dual Codes over the Integers Modulo 4, J. Comb. Theory (A). 62 (1993) 30-45.

[12] J. H. Conway, R. T. Curtis, P. S. Nortan, R. A. Parker and R. A. Wilson, Atlas of the finite Groups, Oxford, U. K. Clarendon Press. (1985).

[13] J. H. Humphreys and M. Y. Prest, Numbers, Groups, and Codes, Cambridge University Press, Cambridge, New York. (1989).

[14] J. H. VanLint and F. J. MacWilliams, Generalised Quadratic Residue Codes, IEEE Trans. Inform. Theory. 24(6) (1978) 730-737.

[15] H. Girrifin, Elementary Theory of Numbers, MaGraw-Hill book Company, New York. (1954).

[16] H. Janwa and A. K. Lal, On the Generalized Hamming Weights of Cyclic Codes, IEEE Trans. Inform. Theory. 43(1) (1997) 299-308.

[17] H. N. Ward, Quadratic Codes of Length 27, IEEE Trans. Inform. Theory. 36(4) (1990) 950-953.

[18] H. N. Ward, Quadratic Residue Codes and Symplectic Groups, Journal of Algerba. 29 (1974) 150-171.

[19] I. F. Blake, Algebraic Coding Theory, History and Developments, Dowdes, Hustechson and Ross, Inc. Stroudsberg. (1973).

[20] I. F. Blake and R. C. Mullin, The Mathematical Theory of Coding, Academic Press, New York. (1975).

[21] Ranjeet Singh, Some Results in the Ring $R_{2p^nq^m} = GF(l)[x]/(x^{2p^nq^m} - 1)$, International Journal of Mathematics Trends and Technology. 35(1) (2016) 32-37.