International Journal of Mathematics Trends and Technology
ISSN: 2231 – 5373 / https://doi.org/10.14445/22315373/IJMTT-V68I4P512

Volume 68 Issue 4, 81-83, April 2022

Original Article

Cyclotomic Cosets in the Ring $R_{8p^n} = GF(l)[x]/(x^{8p^n} - 1)$

Ranjeet Singh

Department of Mathematics, Govt. College, Siwani (Bhiwani).

Received Date: 16 March 2022
Revised Date: 18 April 2022
Accepted Date: 30 April 2022

Abstract - *Explicit expressions for all the 8(nd+1) Cyclotomic Cosets in the ring* $R_{8p^n} = GF(l)[x]/(x^{8p^n} - 1)$*, where p is of the type (8k+1) and l are distinct odd primes* $o(l)_{8p^n} = \phi(8p^n)/d$*,* $(n \geq 1)$ *an intger, are obtained .*

Keywords - *Primitive root; Cyclotomic Cosets. Cyclotomic Number.*

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

I. INTRODUCTION

Let GF(l) be a field of odd prime order l .Let $\eta \geq 1$ be an integer with gcd(l,η)=1.Let $R_\eta = GF(l)[x]/(x^\eta - 1)$ .In this paper, we consider the case when $\eta = 8p^n$ $o(l)_{8p^n} = \phi(8p^n)$/d, (n ≥ 1) where p (8k+1)and l are distinct odd primes . Explicit expressions for all the 8(nd+1) Cyclotomic Cosets in the ring $R_{8p^n} = GF(l)[x]/(x^{8p^n} - 1)$, where p (8k+1) type and l are distinct odd primes $o(l)_{8p^n} = \phi(8p^n)$/d, (n ≥ 1) an intger, are obtained.

II. CYCLOTOMIC COSETS IN $R_{8p^n} = GF(l)[x]/(x^{8p^n} - 1)$

2.1.Remark:- For $0 \leq s \leq \eta - 1$, let $C_s = \{s, sl, sl^2, ..., sl^{t_s - 1}\}$, where t_s is the least positive integer such that $sl^{t_s} \equiv s \pmod{\eta}$ be the cyclotomic coset containing s. corresponding to the cyclotomic coset C_s containing s and its elements are called Cyclotomic Numbers.

Lemma2.1. Let $p..(8k+1)type..and..l$ be distinct odd primes and n ≥ 1, an integer, $o(l)_{8p^n} = \frac{\phi(8p^n)}{d}$.Then $o(l)_{8p^{n-j}} = \frac{\phi(8p^{n-j})}{d}$, for all $0 \leq j \leq n-1$.

Proof . Trivial.

Lemma2.2 There always exists fixed integer g satisfying $(g,8pl) = 1$, 1 < g < 8p, $o(g)_{8p} = \phi(8p)$ and $g^j \not\equiv$,l^k mod(4p) …, $l^{\frac{\phi(8p)}{d}-1}$ and for given distinct odd primes p and l there always exists fixed integer a,b and c satisfying (r, p l) = 1 , 1 < r< 8p, r ≡ t (mod 8p), for 0 ≤ t ≤ φ(8 p) −1 and r= a , b , c and a=2p+1, b=4p+1, c =6p+1, for any j and k and For 0 ≤ j ≤d −1 and For 0 ≤ k ≤ $\frac{\phi(8p)}{d}$ −1.Further for any j , 0 ≤ j ≤ n-1

the set { l, l, l^2 ,l^3 …, $l^{\frac{\phi(8p^{n-i})}{d}-1}$ ………. g^{d-1}, $g^{d-1}l$, $g^{d-1}l^2$, $g^{d-1}l^3$ …, $g^{d-1}l^{\frac{\phi(8p^{n-i})}{d}-1}$ } ,

{r, rl, rl^2 ,rl^3 …, r$l^{\frac{\phi(8p^{n-i})}{d}-1}$ rg,rg l,rg l^2 , rgl^3 …, rg$l^{\frac{\phi(8p^{n-i})}{d}-1}$ rg^2, rg^2l, rg^2l^2 , rg^2l^3 …, $rg^2l^{\frac{\phi(8p^{n-i})}{d}-1}$ rg^{d-1}, $rg^{d-1}l$, $rg^{d-1}l^2$, $rg^{d-1}l^3$ …,
$rg^{d-1}l^{\frac{\phi(8p^{n-i})}{d}-1}$ } where r=a,b,c forms a reduced residue system modulo $8p^{n-j}$

Proof . Lemma4 [1]

Theorem2.1. If $\eta = 8p^n$ (n ≥ 1), then the 8(nd+1) cyclotomic cosets modulo $8p^n$ are given by

(i) $C_0 = \{0\}, C_{p^n} = \{p^n\}\ C_{2p^n} = \{2p^n\}, C_{3p^n} = \{3p^n\}$,

$C_{4p^n} = \{4p^n\}$, $C_{5p^n} = \{5p^n\}$, $C_{6p^n} = \{6p^n\}$, $C_{7p^n} = \{7p^n\}$

For $0 \le k \le d-1$ and For $0 \le i \le n-1$

(i) $C_{g^k p^i} = \{g^k p^i,\ g^k p^i l, \ldots, g^k p^i l^{\frac{\phi(8p^{n-i})}{d}-1}\}$,

(ii) $C_{2g^k p^i} = \{2g^k p^i,\ 2g^k p^i l, \ldots, 2g^k p^i l^{\frac{\phi(8p^{n-i})}{d}-1}\}$,

(iii) $C_{4g^k p^i} = \{4g^k p^i,\ 4g^k p^i l, \ldots, 4g^k p^i l^{\frac{\phi(8p^{n-i})}{d}-1}\}$,

(iv) $C_{8g^k p^i} = \{8g^k p^i,\ 8g^k p^i l, \ldots, 8g^k p^i l^{\frac{\phi(8p^{n-i})}{d}-1}\}$,

(v) $C_{ag^k p^i} = \{ag^k p^i,\ ag^k p^i l, \ldots, ag^k p^i l^{\frac{\phi(8p^{n-i})}{d}-1}\}$,

(vi) $C_{2ag^k p^i} = \{2ag^k p^i,\ 2ag^k p^i l, \ldots, 2ag^k p^i l^{\frac{\phi(8p^{n-i})}{d}-1}\}$,

(vii) $C_{bg^k p^i} = \{bg^k p^i,\ bg^k p^i l, \ldots, bg^k p^i l^{\frac{\phi(8p^{n-i})}{d}-1}\}$,

(viii) $C_{cg^k p^i} = \{cg^k p^i,\ cg^k p^i l, \ldots, cg^k p^i l^{\frac{\phi(8p^{n-i})}{d}-1}\}$,

Where a,b,c and g are defined as in lemma2.2.

Proof. $C_0 = \{0\}, C_{p^n} = \{p^n\}\ C_{2p^n} = \{2p^n\}, C_{3p^n} = \{3p^n\}\ C_{4p^n} = \{4p^n\}$,

$C_{5p^n} = \{5p^n\}$, $C_{6p^n} = \{6p^n\}$, $C_{7p^n} = \{7p^n\}$

are trivial.For $0 \le k \le d-1$ and For $0 \le i \le n-1$Since by our choice $o(l)_{8p^{n-j}} = \frac{\phi(8p^{n-j})}{d}$ Hence $C_{g^k p^i}$ is the cyclotomic coset containing $g^k p^i$. Similarly $C_{2g^k p^i}$ is the cyclotomic coset containing $2g^k p^i$ .On same lines we can say that and $C_{4g^k p^i}$ are the cyclotomic coset containing $4g^k p^i$.

Similarly we can prove for the cyclotomic cosets $C_{ag^k p^i}$ and so on.

We now claim that the cyclotomic cosets obtained in (i)-(viii) above are the only cyclotomic cosets modulo $8p^n$.

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

$|C_0|=1, |C_{p^n}|=1, |C_{2p^n}|=1, |C_{4p^n}|=1$‘ $|C_{3p^n}|=1, |C_{5p^n}|=1$

, $|C_{6p^n}|=1, |C_{7p^n}|=1$For $0 \le k \le d-1$ and For $0 \le i \le n-1$

$|C_{g^k p^i}|, |C_{2g^k p^i}|$, , and $|C_{4g^k p^i}| = \frac{\phi(8p^{n-i})}{d}$

Similarly we can cheque for the cyclotomic cosets $C_{ag^k p^i}$ and so on.

Then, by order considerations, it follows that the sum :

$|C_0| + |C_{p^n}| + |C_{2p^n}| + |C_{4p^n}| + |C_{3p^n}| + |C_{5p^n}| + |C_{6p^n}| + |C_{7p^n}|$

$$+\left|\sum_{k=0,i=0}^{d-1,n-1} g^k p^i\right| + \left|\sum_{k=0,i=0}^{d-1,n-1} 2g^k p^i\right| + \left|\sum_{k=0,i=0}^{d-1,n-1} 4g^k p^i\right| + \left|\sum_{k=0,i=0}^{d-1,n-1} 8g^k p^i\right|$$

$$+\left|\sum_{k=0,i=0}^{d-1,n-1} ag^k p^i\right| + \left|\sum_{k=0,i=0}^{d-1,n-1} 2ag^k p^i\right| + \left|\sum_{k=0,i=0}^{d-1,n-1} bg^k p^i\right| + \left|\sum_{k=0,i=0}^{d-1,n-1} cg^k p^i\right|$$

$$= 8 + 8\sum_{,i=0}^{,n-1} \frac{\phi(8p^{n-i})}{d} = 8 + 8\,(p^n - 1) = 8p^n$$

III. 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 8(nd+1) Cyclotomic Cosets are obtained in the ring $R_{8p^n} = GF(l)[x]/(x^{8p^n} - 1)$, 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] M.Raka, G.K. Bakshi, A. Sharma V.C. Dumir, Cyclotomic Numbers and Primitive Idempotents in the Ring $R_{p^n} = GF(l)[x]/(x^{p^n} - 1)$, Finite Field & Their Appl. 3(2) (2004) 653-673.

[2] S.K. Arora, M. Pruthi, Minimal Cyclic Codes of Prime Power Length, Finite Fields Appl. 3 (1997) 99-113.

[3] S.K. Arora, M. Pruthi, Minimal Cyclic Codes of Length $2p^n$, Finite Fields Appl. 5 (1999) 177-187.

[4] 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.

[5] G.K.Bakshi, Madhu Raka, Minimal Cyclic Codes of Length $p^n q$, Finite Fields Appl. 9 (2003) 432-448.

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

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

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

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

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

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

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

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

[14] I.N. Herstein, Non-Commutative Rings, Carus Math. Monographs, Math. Assoc. Amer. (15) (1968).

[15] I. S. Reed, A Class of Multiple Error Correcting Codes and the Decoding Scheme, IRE Trans. on Inform. Theory, IT. (4) (1954) 38-49.

[16] Ian F. Blare, Distance Properties of the Group Code of Gaussian Channel, SIAM J. Appl. Math. 23 (1972) 312-324.

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

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

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

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

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

[22] 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).

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

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