Cyclotomic Cosets in The Ring R_(2p^n q^m)=GF(l) [x]/(x^(2p^n q^m)-1)

by Jana Publication & Research

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

ABSTRACT

We consider the ring $R_{2p^nq^m} = GF(l)[x]/(x^{2p^nq^m} - 1)$ 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 $2(m \times n \times d + m + n + 1)$ Cyclotomic Cosets are obtained, p does not divide $q - 1$.

Keywords: Cyclotomic coset, generating polynomials, and minimal cyclic codes.

MSC: Primary 11T30; Secondary 94 B15, 11T 71.

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 $R_z = GF(l)[x]/(x^z - 1)$. The minimal cyclic codes of length z over $GF(l)$ are ideals of the ring R_z. G.K. Bakshi and Madhu Raka [4] obtained $3n + 2$primitive idempotents in $R_z$for $z = p^nq$ 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 $z = p^nq$ 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], we obtain all the results of [4]. So [4] becomes a special case of [5].

In this paper, we consider the case when Z=$2p^nq^m$ 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 2($m \times n \times d + m + n + 1$) Cyclotomic Cosets are obtained. $gcd(\varphi(p^n), \varphi(q^m)) = d$, p does not divide $q - 1$ .. Here, we extend the results of Amita Sahni and P.T. Sehgal [5].

REMARK2.1 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 $sl^{t_s} \equiv s$ (mod2 p^nq^m) be the cyclomic coset containing s.

LEMMA2.1. Let p, q, l be distinct odd primes, n ≥ 1 an integer,$o(l)_{2p^{n-j}} = \varphi(2p^{n-j})$, $o(l)_{q^{m-k}} = \varphi(q^{m-k})$ and $gcd(\varphi(2p^{n-j}), \varphi(q^{m-k})) = d$ then$o(l)_{2p^{n-j}q^{m-k}} = \frac{\varphi(2p^{n-j}q^{m-k})}{d}$, for all $0 \leq j \leq n - 1$ and $0 \leq k \leq m - 1$.

Proof. Let $o(l)_{2p^{n-j}q^{m-k}} = t$, 0 ≤ j ≤ n – 1and $0 \leq k \leq m - 1$.Then $l^t \equiv 1 \, mod \, 2p^{n-j} \, q^{m-k}$But *p* and *q* are distinct odd primes. Hence $l^t \equiv 1 \, mod \, 2p^{n-j}$and $l^t \equiv 1 \, mod \, q^{m-k}$.Since $o(l)_{p^{n-j}} = \varphi(2p^{n-j})$ and, $o(l)_{q^{m-k}} = \varphi(q^{m-k})$ therefore, $\varphi(2p^{n-j})$ and $\varphi(q^{m-k})$ divides t.Then $lcm(\varphi(2p^{n-j}), \varphi(q^{m-k})) = \frac{\varphi(2p^{n-j}q^{m-k})}{d}$ 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 $l^{\varphi(\frac{2p^{n-j}q^{m-k}}{d})} \equiv 1 \, mod \, q^{m-k}$.Similarly, $l^{\varphi(\frac{2p^{n-j}q^{m-k}}{d})} \equiv 1 \, mod \, p^{n-j}$. As *p* and *q* are distinct primes, therefore, we get $l^{\varphi(\frac{2p^{n-j}q^{m-k}}{d})} \equiv 1 \, mod \, 2p^{n-j} \, q^{m-k}$

Hence, $t = o(l)_{2p^{n-j}q^{m-k}}$divides $\frac{\varphi(2p^{n-j}q^{m-k})}{d}$ and we get that $t = \frac{\varphi(2p^{n-j}q^{m-k})}{d}$.

LEMMA2.2. For given p, q, l distinct odd primes such that *gcd* $(\varphi(p),\varphi(q))=d$, and *l* is a primitive root mod(*p)* as well as *q,* then there always exists a fixed integer a satisfying gcd(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,a², a³ ,……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, …, $l^{\frac{\varphi(2p^{n-j}q^{m-k})}{d}-1}$, a, a$l$, …,a$l^{\frac{\varphi(2p^{n-j}q^{m-k})}{d}-1}$, a² , a²$l$, a²$l^2$, …, a²$l^{\frac{\varphi(2p^{n-j}q^{m-k})}{d}-1}$, a^{d-1} , a^{d-1} l, …, a^{d-1} $l^{\frac{\varphi(2p^{n-j}q^{m-k})}{d}-1}$} forms a reduced residue system modulo $2p^{n-j}q^{m-k}$.

Proof. Trivial

THEOREM2.1. If $\eta = 2p^nq^m$ (m and n ≥ 1), Then the $2(m \times n \times d + m + n + 1)$ cyclotomic cosets modulo $2p^nq^m$ are given by (i) C_0= {0} , $(ii) C_{p^nq^m}$= {p^nq^m } (iii) for $0 \le k \le m-1$

C_{p^n}= {p^n, $p^n l$, …, $p^n l^{\varphi(q^{m-k})-1}$} , $(iv) C_{2p^n}$= {$2p^n$, $2p^n l$, …, $2p^n l^{\varphi(q^{m-k})-1}$} and for $0 \le j \le n-1$,

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

(vi)C_{2q^m}= {$2q^m$,$2q^m l$, …, $2q^m l^{\varphi(p^{n-j})-1}$}

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

(vii)$C_{a^wp^jq^k}$={ $a^wp^jq^k$,$a^wp^jq^k l$, …,$a^wp^jq^k$ $l^{\frac{\varphi(2p^{n-j}q^{m-k})}{d}-1}$} , $(viii)$ $C_{2a^wp^jq^k}$={ $2a^wp^jq^k$,$2a^wp^jq^k l$, …,$2a^wp^jq^k$ $l^{\frac{\varphi(2p^{n-j}q^{m-k})}{d}-1}$} where the number a is given by Lemma 2.2.

Proof: Trivial as Lemma 2.2.

5. 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 2pⁿ" 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 $p^n q$", Finite Fields Appl. 9 (2003) 432-448.

[5] A.Sahni and P.T.Sehgal,"Minimal Cyclic Codes of length pnq," 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).

Cyclotomic Cosets in The Ring R_(2p^n q^m)=GF(l)[x]/(x^(2p^n q^m)-1)

ORIGINALITY REPORT

29%	27%	26%	3%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	ijmttjournal.org Internet Source	12%
2	core.ac.uk Internet Source	8%
3	www.m-hikari.com Internet Source	4%
4	m.moam.info Internet Source	2%
5	Sahni, Amita, and Poonam Trama Sehgal. "Minimal cyclic codes of length", Finite Fields and Their Applications, 2012. Publication	2%
6	Pinki Devi, Pankaj Kumar. "CYCLOTOMIC COSETS MODULO m", JP Journal of Algebra, Number Theory and Applications, 2021 Publication	1%

Exclude quotes	On	Exclude matches	Off
Exclude bibliography	On		