International Journal of Mathematics Trends and Technology
ISSN: 2231 – 5373 /doi:10.14445/22315373/IJMTT-V67I4P513
Volume 67 Issue 4, 96-100, April, 2021

Cyclotomic Numbers In The Ring $R_{8p^nq} = GF(l)[x]/(x^{8p^nq} - 1)$ (n ≥ 1)

Dr. Ranjeet Singh
Assistant Professor Mathematics, Govt. College, Siwani (Bhiwani), Haryana

Explicit expressions for all the 24n+9 Cyclotomic numbers in the ring $R_{8p^nq} = GF(l)[x]/(x^{8p^nq} - 1)$ *, where p, q, l are distinct odd primes* $o(l)_{8p^n} = \phi(8p^n)/2$*, (n ≥ 1) and* $o(l)_q = \phi(q)/2$ *with gcd* $(\phi(8p^n)/2, \phi(q)/2) = 1$*, are obtained.*

I. INTRODUCTION

Let GF(l) be a field of odd prime order l .Let m ≥ 1 be an integer with gcd(l,m)=1.Let $R_m = GF(l)[x]/(x^m - 1)$ .The minimal cyclic codes of length m over GF(l) are the ideals of the ring R_m generated by the primitive idempotents.For $m = 2$, 4 , p^n, $2p^n$, p an odd prime and l *is* primitive root mod(m) the primitive idempotent in R_m have been obtained by Arora and Pruthi [1,2] .

When $m = p^n q$ where p, q are distinct odd primes and l is a primitive root mod p^n and q both with gcd ($\phi(p^n)/2$, $\phi(q)/2$) = 1, the primitive idempotent in R_m have been obtained by, G.K.Bakshi and Madhu Raka 4.

In this paper, we consider the case when $m = 8p^n q$ where p, q are distinct odd primes

and $o(l)_{8p^n} = \phi(8p^n)/2$,(n ≥ 1) and $o(l)_q = \phi(q)/2$, with gcd ($\phi(8p^n)/2, \phi(q)/2$)=1.We obtain explicit expressions for all the 6n+3 *Cyclotomic numbers* in R_{8p^nq}

Throughout in this paper we assume that p,q, l are distinct odd primes, $o(l)_{8p^n} = \phi(8p^n)/2$,(n ≥ 1) and $o(l)_q = \phi(q)/2$, with gcd ($\phi(8p^n)/2$, $\phi(q)/2$) = 1.

LEMMA 2.1. Let p,q,l be distinct odd primes, n ≥ 1 an integer, $o(l)_{8p^{n-j}} = \frac{\phi(8p^{n-j})}{2}$, $o(l)_q = \frac{\phi(q)}{2}$ and gcd $\left(\frac{\phi(8p^{n-j})}{2}, \frac{\phi(q)}{2}\right)$ =1, then $o(l)_{8p^{n-j}q} = \frac{\phi(8p^{n-j}q)}{4}$, for all j, 0 ≤ j ≤ n − 1.

Proof. Trivial**.**

LEMMA 2.2. For given p, q, l distinct odd primes, there always exists fixed integers a and b satisfying gcd(a, 8pq$l$)=1, gcd(b, 8pq$l$)=1,1 < a < 8pq, a $\not\equiv l^k \pmod{8pq}$, where $0 \le k \le \frac{\phi(8pq)}{4} - 1$ and b $\not\equiv r l^k \pmod{8pq}$, where $0 \le k \le \frac{\phi(8pq)}{4} - 1$ and $r = a$ or 1, such that, for $0 \le j \le n-1$,the set {1 , l , l^2, …, $l^{\frac{\phi(8p^{n-j}q)}{4}-1}$, a, al , …,a$l^{\frac{\phi(8p^{n-j}q)}{4}-1}$, b ,bl , bl^2, …, b$l^{\frac{\phi(8p^{n-j}q)}{4}-1}$, ab, ab$l$, …,ab$l^{\frac{\phi(8p^{n-j}q)}{4}-1}$ } forms a reduced residue system modulo $8p^{n-j}q$ and the set {1 , l, l^2, ..,

$l^{\frac{\phi(8p^{n-j})}{2}-1}$, g, gl, …, g $l^{\frac{\phi(8p^{n-j})}{2}-1}$} forms a reduced residue system modulo $8p^{n-j}$ where $g = a$ or b and {1 , l, l^2, .., $l^{\frac{\phi(q)}{2}-1}$, g, gl, …, g $l^{\frac{\phi(q)}{2}-1}$} forms a reduced residue system modulo q where $g = a$ or b.

Proof . By Lemma 2.1, $o(l)_{8pq} = \frac{\phi(8pq)}{4}$ therefore, the numbers 1 , l, l^2, …, $l^{\frac{\phi(8pq)}{4}-1}$ are all incongruent (mod 8pq).As the order of the reduced residue system modulo pq is ϕ(pq), therefore, we can choose a number a satisfying gcd(a, pq$l$) =1, 1 < a < pq, a $\not\equiv l^k$ (mod pq), for $0 \le k \le \frac{\phi(pq)}{4} - 1$. Now again The $\frac{\phi(pq)}{2}$ numbers $\{1, l, l^2, ...l^{\frac{\phi(pq)}{4}-1}, a, al, al^2, ...al^{\frac{\phi(pq)}{4}-1}\}$ are all incongruent mod(pq).But reduced residue system modulo pq contains exactly ϕ(pq) numbers.Therefore there exist again a fixed integer b such that gcd(b, pq$l$) =1, and b $\not\equiv r l^k$ (mod pq), where $0 \le k \le \frac{\phi(pq)}{4} - 1$ and $r = a$ or 1, such that, for $0 \le j \le n - 1$,the set { 1, l , l^2, …, $l^{\frac{\phi(pq)}{4}-1}$, a, al , …,a$l^{\frac{\phi(pq)}{4}-1}$, b ,bl , bl^2, …, b$l^{\frac{\phi(pq)}{4}-1}$, ab, ab$l$, …,ab $l^{\frac{\phi(pq)}{4}-1}$} containing ϕ(pq) incongruent numbers forms a reduced residue system modulo pq . Since for $0 \le k \le \frac{\phi(pq)}{4} - 1$, a $\not\equiv l^k$ (mod pq), and b $\not\equiv r l^k$ (mod pq), where $r = a$ or 1, it then follows easily that, a $\not\equiv l^k$ (mod p^{n-j} q) , and b$\not\equiv r l^k$ (mod p^{n-j} q) for $0 \le k \le \frac{\phi(p^{n-j}q)}{4} - 1$, where $r = a$ or 1. Hence the set {1 , l , l^2, …, $l^{\frac{\phi(8p^{n-j}q)}{4}-1}$, a, a$l$, …,a $l^{\frac{\phi(8p^{n-j}q)}{4}-1}$, b ,b$l$, bl^2, …, b$l^{\frac{\phi(8p^{n-j}q)}{4}-1}$, ab, ab$l$, …,ab$l^{\frac{\phi(8p^{n-j}q)}{4}-1}$} forms a reduced residue system modulo $8p^{n-j}q$.

On the similar lines we also get that the set {1, l, l^2, .., $l^{\frac{\phi(8p^{n-j})}{2}-1}$, g, g$l$, …, g $l^{\frac{\phi(8p^{n-j})}{2}-1}$} forms a reduced residue system modulo $8p^{n-j}$ where $g = a$ or b ,and {1 , l, l^2, .., $l^{\frac{\phi(q)}{2}-1}$, g, gl, …, g $l^{\frac{\phi(q)}{2}-1}$} forms a reduced residue system modulo q where g=a or b.

REMARK 2.2. Since in Lemma2.2 we have a $\not\equiv l^k$ (mod pq), and b$\not\equiv r l^k$ (modpq), where $0 \le k \le \frac{\phi(pq)}{4} - 1$ and $r = a$ or 1.Then mainly the following cases holds: For $0 \le s \le \frac{\phi(pq)}{4} - 1$, we have Case (i) a $\equiv l^s$ (modp), b $\equiv l^s$ (modq), b $\not\equiv l^s$ (modp) and a $\not\equiv l^s$ (modq).

Case (ii) a $\equiv l^s$ (modq), b$\equiv l^s$ (modp), b $\not\equiv l^s$ (modq) and a $\not\equiv l^s$ (modp).

Case (iii) a$\not\equiv l^s$ (modp), b$\equiv l^s$ (modq), b$\not\equiv l^s$ (modp) and a$\not\equiv l^s$ (modq).

Case (iv) a $\not\equiv l^s$ (modp), a $\equiv l^s$ (modq), b $\not\equiv l^s$ (modp) and b $\not\equiv l^s$ (modq).Here we are considering the case (i) because the remaining cases follows in a similar way.

Also in case (i) q $C_q = C_q$ or q $C_q = C_{bq}$ and we are considering the case when q $C_q = C_q$.

THEOREM 2.3. If $\eta = 8p^nq$ ($n \geq 1$), then the $24n+9$ cyclotomic cosets modulo $8p^nq$ are given by (i) $C_0 = \{0\}$ (ii)

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

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

$C_{4p^n} = \{4p^n, 4p^n l, \ldots, 4p^n l^{\frac{\phi(q)}{2}-1}\}$

$C_{8p^n} = \{8p^n, 8p^n l, \ldots, 8p^n l^{\frac{\phi(q)}{2}-1}\}$

(iii) $C_{ap^n} = \{ap^n, ap^n l, \ldots, ap^n l^{\frac{\phi(q)}{2}-1}\}$

$C_{2ap^n} = \{2ap^n, 2ap^n l, \ldots, 2ap^n l^{\frac{\phi(q)}{2}-1}\}$

$C_{4ap^n} = \{4ap^n, 4ap^n l, \ldots, 4ap^n l^{\frac{\phi(q)}{2}-1}\}$

$C_{8ap^n} = \{8ap^n, 8ap^n l, \ldots, 8ap^n l^{\frac{\phi(q)}{2}-1}\}$

and for $0 \leq j \leq n-1$, (iv) $C_{p^jq} = \{p^jq, p^jql, \ldots, p^j q\, l^{\frac{\phi(p^{n-j})}{2}-1}\}$

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

$C_{4p^jq} = \{4p^jq, 4p^jql, \ldots, 4p^j q\, l^{\frac{\phi(p^{n-j})}{2}-1}\}$

$C_{8p^jq} = \{8p^jq, 8p^jql, \ldots, 8p^j q\, l^{\frac{\phi(p^{n-j})}{2}-1}\}$

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

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

C_{4bp^jq} ={4bp^{j}q, 4bp^{j}ql, …,4 bp^j $l^{\frac{\phi(p^{n-j})}{2}-1}$ }

C_{8bp^jq} ={8bp^{j}q,8 bp^{j}ql, …, 8bp^j $l^{\frac{\phi(p^{n-j})}{2}-1}$ }

, (vi) C_{p^j} ={p^j, p^{j}l, …, p^j $l^{\frac{\phi(8p^{n-j}q)}{4}-1}$ }

C_{2p^j} ={2p^j, 2p^{j}l, …, 2p^j $l^{\frac{\phi(8p^{n-j}q)}{4}-1}$ }

C_{4p^j} ={4p^j,4 p^{j}l, …, 4p^j $l^{\frac{\phi(8p^{n-j}q)}{4}-1}$ }

C_{8p^j} ={8p^j,8 p^{j}l, …, 8p^j $l^{\frac{\phi(8p^{n-j}q)}{4}-1}$ }

(vii) C_{bp^j} ={bp^j, bp^j l, …, bp^j $l^{\frac{\phi(8p^{n-j}q)}{4}-1}$ },

C_{2bp^j} ={2bp^j, 2bp^j l, …, 2bp^j $l^{\frac{\phi(8p^{n-j}q)}{4}-1}$ },

C_{4bp^j} ={4bp^j,4 bp^j l, …,4 bp^j $l^{\frac{\phi(8p^{n-j}q)}{4}-1}$ },

C_{8bp^j} ={8bp^j, 8bp^j l, …, 8bp^j $l^{\frac{\phi(8p^{n-j}q)}{4}-1}$ },

(viii) C_{ap^j} ={ap^j, ap^{j}l, …, ap^j $l^{\frac{\phi(8p^{n-j}q)}{4}-1}$ }

C_{2ap^j} ={2ap^j, 2ap^{j}l, …, 2ap^j $l^{\frac{\phi(8p^{n-j}q)}{4}-1}$ }

C_{4ap^j} ={4ap^j, 4ap^{j}l, …, 4ap^j $l^{\frac{\phi(8p^{n-j}q)}{4}-1}$ }

$C_{8ap^j} = \{8ap^j, 8ap^j l, \ldots, 8ap^j l^{\frac{\phi(8p^{n-j}q)}{4}-1}\}$

(ix) $C_{abp^j} = \{abp^j, abp^j l, \ldots, abp^j l^{\frac{\phi(8p^{n-j}q)}{4}-1}\}$

$C_{2abp^j} = \{2abp^j, 2abp^j l, \ldots, 2abp^j l^{\frac{\phi(8p^{n-j}q)}{4}-1}\}$

$C_{4abp^j} = \{4abp^j, 4abp^j l, \ldots, 4abp^j l^{\frac{\phi(8p^{n-j}q)}{4}-1}\}$

$C_{8abp^j} = \{8abp^j, 8abp^j l, \ldots, 8abp^j l^{\frac{\phi(8p^{n-j}q)}{4}-1}\}$

.where the numbers a and b are given by Lemma2.2.

Proof . Trivial**.**

REFERENCES

[1] Arora S.K., M. Pruthi, Minimal cyclic codes of prime power length", Finite Fields Appl., **3**(1997), 99-113.

[2] Arora.S.K., M. Pruthi, Minimal cyclic codes of length $2p^n$", Finite Fields Appl., **5** (1999), 177-187.

[3] Anuradha Sharma, Bakshi.G.K. Dumir V.C., 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] Bakshi G.K., Madhu Raka, Minimal cyclic codes of length $p^n q$, Finite Fields Appl., **9**(2003), 432-448.

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

[6] F. J. Macwilliams and N. J. A. Sloane, The Theory of Errer Correcting Codes, North Holland, Amsterdam, 1977.