International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

COPY RIGHT

2020 IJIEMR.Personal use of this material is permitted. Permission from IJIEMR must be obtained for all other uses, in any current or future media, including reprinting/republishing this material for advertising or promotional purposes, creating new collective works, for resale or redistribution to servers or lists, or reuse of any copyrighted component of this work in other works. No Reprint should be done to this paper, all copy right is authenticated to Paper Authors

IJIEMR Transactions, online available on 27th Nov 2020. Link :http://www.ijiemr.org/downloads.php?vol=Volume-09&issue=ISSUE-12

DOI: 10.48047/IJIEMR/V09/I12/81

Title: **A Gist of Analogues µ_pto Mobius function µ**

Volume 09, Issue 12, Pages: 428-429

Paper Authors

Oduri Thrinadh

USE THIS BARCODE TO ACCESS YOUR ONLINE PAPER

To Secure Your Paper As Per UGC Guidelines We Are Providing A Electronic Bar Code

International Journal for Innovative Engineering and Management Research
A Peer Revieved Open Access International Journal
www.ijiemr.org

A Gist of Analogues μ_p to Mobius function μ

Oduri Thrinadh[1]

[1]Department of Mathematics, Welfare Engineering College, Visakhapatnam, AP, India
E-Mail: oduri65@gmail.com

ABSTRACT

If $f(x) \in Z_p[x]$ is an irreducible polynomial, the number of polynomials $g(x)$ with $deg(g(x)) \le deg(f(x)) \ni (g(x), f(x)) = 1$ is the order of the multiplicative group of $Z_p[x]/(f(x))$. In this paper we introducing analogues μ_p to Mobius function μ defined on $\wp Z_p[x]$, the set of all primitive polynomials in $Z_p[x]$.

Keywords: FINITE FIELD, PRIMITIVE POYLNOMIALS.

1. INTRODUCTION

In the construction of cryptosystems with polynomials in $Z_p[x]$ for prime p, the quotient ring of the polynomial ring in $Z_p[x]$ with an ideal generated by $(f(x))$, for $f(x)$ a polynomial in $Z_p[x]$ is considered and the group of units of this quotient is taken as the message space.

In this paper we introducing analogues μ_p to Mobius function μ defined on $\wp Z_p[x]$, the set of all primitive polynomials in $Z_p[x]$.

We introduce the functions μ_p on $\wp Z_p[x]$ and prove one result relating μ_p in the following section.

Definition of Mobius functtion $\mu(n)$:

The mobius function μ is defined as $\mu(1) = 1$, if $n>1$, where $n = {p_1}^{a1} \ldots {p_k}^{ak}$ then $\mu(n) = \begin{cases} (-1)^k & \text{if } a_1 = a_2 = \cdots = a_k = 1 \\ 0 & \text{otherwise} \end{cases}$

Note that $\mu(n) = 0$ if and only if 'n' has a square factor >1

Here is a short table of valuees of $\mu(n)$.

Theorem:- if $n \ge 1$, we have $\sum_{d/n} \mu(d) = \left[\frac{1}{n}\right] = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } n > 1 \end{cases}$.

Proof: The formula is clearly true if $n = 1$

Now assume, then that $n > 1$ and write $n = {p_1}^{a1} \ldots {p_k}^{ak}$

In the sum $\sum_{d/n} \mu(d)$ the only non zero terms comes from $d = 1$ and from thosee divisors of 'n' which are products of distinct primes.

Thus,

$$\sum_{d/n} \mu(d) = \mu(1) + \mu(p_1) + \cdots + \mu(p_k) + \mu(p_1 p_2) + \cdots + \mu(p_{k-1} p_k) + \cdots \mu(p_1 p_2 \ldots p_k)$$
$$= 1 + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k$$
$$= (1-1)^K = 0$$

Hence proved

2. μ ANALOGUES IN $Z_p[x]$

In this section we define two functions μ_p on $\wp Z_p[x]$ that analogue to the arithmetical functions Mobius function $\mu(n)$.

2.1 μ_p AN ANALOGUE TO MODIUS FUNCTION ON AN $\wp Z_p[x]$

Definition 2.1.1 A real valued function μ_p on $\wp Z_p[x]$ is defined as follows :

$$\mu_p(f(x)) = 1 \text{ if } \deg\ (f(x)) = 0.$$

If $\deg(f(x)) > 0$ and $f = {f_1}^{a_1} {f_2}^{a_2} {f_3}^{a_3} \ldots .. {f_n}^{a_n}$, for $f_i(x)$ irreducible polynomials in $Z_p[x]$,

$$\mu_p(f(x)) = \begin{cases} (-1)^n & if\ a_1 = a_2 = a_3 = ...a_n = 1, \\ 0 & otherwise. \end{cases}$$

Theorem 2.1.2 For $f(x) \in \wp Z_p[x]$ with $deg(f(x)) \geq 0$ we have

$$\sum_{d(x)|f(x)} \mu_p(d(x)) = \begin{cases} 1, if\ deg(f(x)) = 0, \\ 0, if\ deg(f(x)) > 0. \end{cases}$$

Proof. Let $f(x) \in \wp Z_p[x]$, then $f(x)$ is a primitive polynomial. If $deg(f(x)) = 0$, $f(x) = c \in Z_p\ and\ c \neq 0$ further note $c = 1$ as $f(x)$ is primitive. therefore $\sum_{d(x)|f(x)} \mu_p(d(x)) = 1.$

If $deg(f(x)) > 0,$ with $f = f_1^{a_1} f_2^{a_2} f_3^{a_3} \ldots f_r^{a_r}$ and D is the set of divisors of $f(x) \in Z_p[x]$ then for

$$D_1 = \{d(x) : d(x) \mid f(x) \text{ and } d(x) \text{ has no square irreducibl e factor}\} \text{ and}$$

$$D_2 = \{d(x) : d(x) \mid f(x) \text{with } d(x) \text{has a square irreducibl e factor}\}$$

D is given by $\{d(x) \in Z_p[x] : d(x) \mid f(x)\} = D_1 \cup D_2$ and

$$\sum_{d(x)|f(x)} \mu_p(d(x)) = \sum_{\substack{d(x)|f(x) \\ d(x)\in D}} \mu_p(d(x))$$

$$= \sum_{\substack{d(x)|f(x) \\ d(x)\in D_1 \cup D_2}} \mu_p(d(x))$$

$$= \sum_{\substack{d(x)|f(x) \\ d(x)\in D_1}} \mu_p(d(x)) + \sum_{\substack{d(x)|f(x) \\ d(x)\in D_2}} \mu_p(d(x))$$

now as D_1 consists of the factors

$$1, f_1(x), f_2(x), f_3(x), ..., (f_1(x)f_2(x)), (f_1(x)f_3(x)), ...(f_1(x)f_2(x)f_3(x)\ldots f_r(x)),$$

we have $\sum_{d(x)|f(x)} \mu_p(d(x))$

$$= \mu_p(1) + \mu_p(f_1(x)) + ... + \mu_p(f_r(x)) + \mu_p((f_1(x)f_2(x))) + ... + \mu_p((f_1(x)f_2(x)\ldots f_r(x)))$$

$$= 1 + \binom{r}{1}(-1) + \binom{r}{2}(-1)^2 + ... + \binom{r}{r}(-1)^r$$

$$= (1-1)^r = 0$$

$$\sum_{d(x)|f(x)} \mu_p(d(x)) = 0 \text{ if } deg(f(x)) > 0.$$

Therefore $\sum_{d(x)|f(x)} \mu_p(d(x))$ =0 $if\ \ deg(f(x)) > 0.$

\

3.CONCLUSION

This formula for $\phi_p(f(x))$ gives the order of the multiplicative group $Z_p[x]/(f(x))$ for $f(x)$ any primitive polynomial in $Z_p[x]$; This product formula developed is quite useful in the construction of cryptosystem with polynomial in $Z_p[x]/(f(x))$, with the group of units of the quotient $Z_p[x]/(f(x))$ as message space.

REFERENCES

[1] Tom M. Apostol, Introduction to analytic number theory (New york: Springer-Verlag,1989) 24-28.

[2] Rudolf Lidl, Aapplied abstract algebra((New york: Springer-Verlag,1984) 144-153.

[3] Gary L.Muller, Carl Mummert, Jhon Polking Finite fields and appilications (USA: American Mathematical Society, 2007) 1-13.

[4] P.B.Battacharya, S.K.Jain and S.R.Nagpaul, Basic abstract algebra, (Cambridge: Cambridge university press,1995) 310-315.

[5] Alina Carmen Cojocaru and M.RamMurty, An introduction to sieve methods and their applications (Cambridge: Cambridge University Press, 2005) 2-4.

[6] James. J.Tattersall, Elementary number theory in nine chapters (Cambridge: Cambridge University Press, 2005) 173-179.

[7] Kenneth Ireland and Michael Rosen, A classical introduction to modern number theory (New york: Springer-Verlag, 1972) 19-20, 79-85.

[8] Victor Shoup, A computational introduction to number theory and algebra (Cambridge: Cambridge University Press, 2005) 24-29.

[9] David M.Burton, Elementary number theory (New Delhi: Universal Bookstall, 1989) 156-160.