International Research Journal of Mathematics, Engineering and IT
Vol. 3, Issue 9, September 2016 IF- 3.563 ISSN: (2349-0322)

Website: www.aarf.asia Email : editor@aarf.asia , editoraarf@gmail.com

COUNTING IN $Z_p[x]$

[1]P. Anuradha Kameswari, [2]Y. Swathi
Department of Mathematics, Andhra University,
Visakhapatnam - 530003, Andhra Pradesh, India.

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 propose a formula for this order in the case when $f(x)$ is any primitive polynomial. We arrive at this formula by introducing analogues μ_p and ϕ_p to Mobius and Euler functions μ and ϕ defined on $\wp Z_p[x]$, the set of all primitive polynomials in $Z_p[x]$.

Key words *: 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 context it is important to compute the order of this group. If $f(x)$ is an irreducible polynomial then $Z_p[x]/(f(x))$ is a field and the group of units has $p^k - 1$ elements, for $k = deg(f(x))$, [1] [11]. This group of units is given by the set $\{g(x) \in Z_p[x] : deg(g(x)) < deg(f(x)) \ni (g(x), f(x)) = 1\}$, as for any $g(x) \in Z_p[x]/(f(x))$, $g(x)$ is invertible if and only if $deg(g(x)) < deg(f(x))$ and $gcd(g(x), f(x)) = 1$. [8]

In this paper we propose a formula for the order of group of units in $Z_p[x]/(f(x))$, for

$f(x)$ any primitive polynomial in $Z_p[x]$, we denote this order by $\phi_p(f(x))$ and we prove this result for $f(x)$ that are not irreducible as well. We develop the formula for $\phi_p(f(x))$ by using the analogues μ_p and ϕ_p to Mobius function μ and Euler function ϕ respectively.[2][3][9] We introduce the functions μ_p and ϕ_p on $\wp Z_p[x]$ and prove some results relating μ_p and ϕ_p in the following section.

2 μ and ϕ analogues in $Z_p[x]$:

In this section we define two functions μ_p and ϕ_p on $\wp Z_p[x]$ that are analogues to the arithmetical functions Mobius function $\mu(n)$ and Euler function $\phi(n)$

2.1 μ_p an analogue to Mobius function on $\wp Z_p[x]$:

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

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

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 $f = f_1^{a_1} f_2^{a_2} f_3^{a_3} \dots f_r^{a_r}$ and D is the set of divisors of $f(x) \in Z_p[x]$ then for

$D_1 = \{d(x) : d(x) | f(x) \text{ and } d(x) \text{ has no square irreducible factor}\}$ and

$D_2 = \{d(x) : d(x) | f(x) \text{with } d(x) \text{has a square irreducible factor}\}$

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

$1, f_1(x), f_2(x), f_3(x), \dots\dots, (f_1(x) f_2(x)), (f_1(x) f_3(x)), \dots\dots. (f_1(x) f_2(x) f_3(x) \dots f_r(x)),$ we have

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

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

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

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

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

2.2 ϕ_p an Analogue to Euler function ϕ on $\wp Z_p[x]$:

Definition 2.2.1 we define a function ϕ_p on $\wp Z_p[x]$ follows:

For any $f(x) \in \wp Z_p[x]$,

$\phi_p(f(x)) = 1$ if $deg(f(x)) = 0$;

If $deg(f(x)) > 0$.

Then $\phi_p(f(x))$ is the number of polynomials $g(x) \in Z_p[x]$ such that $deg(g(x)) < deg(f(x))$ and $(g(x), f(x)) = 1$.

$$\text{Note: } \phi_p(f(x)) = \sum_{\substack{i=1 \\ g(x)\in k_f \\ (g(x), f(x))}}^{n} 1 \text{ where } k_f = \{g(x) \in Z_p[x] : deg(g(x)) < deg(f(x))\},$$

Theorem 2.2.2 For $deg(f(x)) \geq 1$ we have

$$\phi_p(f(x)) = \sum_{d(x)|f(x)} \mu_p(d(x)).\frac{p^{deg(f(x))}}{p^{deg(d(x))}}$$

Proof. Let $k_f = \{g(x) \in Z_p[x] : deg(g(x)) < deg(f(x))\}$.

And note if $deg(f(x)) = s$, then for all $g(x) \in Z_p[x], deg(g(x)) \leq s.$

we have $g(x) = a_0 + a_1 x + \ldots + a_{s-1} x^{s-1}$ for $a_i \in Z_p \forall\, 0 \leq i \leq s$

Now as the number of k_f has p^s elements[8]

Possible sequences $(a_0, a_1, a_2, \ldots, a_{s-1}) = p^s$

$$\phi_p(f(x)) = \sum_{\substack{g_i(x)\in k_f \\ (g_i(x), f(x))=1}} 1$$

$$= \sum_{\substack{i=1 \\ (g_i(x), f(x))=1}}^{p^s} 1$$

$$= \sum_{i=1}^{p^s} \sum_{d(x)|(g_i(x), f(x))} \mu_p(d(x)) \quad (By\ theorem\ 2.1.2)$$

$$= \sum_{i=1}^{p^s} \sum_{\substack{d(x)|g_i(x) \\ d(x)|f(x)}} \mu_p(d(x))$$

$$= \sum_{d(x)|f(x)} \sum_{i=1}^{p^{deg(f(x))-deg(d(x))}} \mu_p d(x)$$

$$= \sum_{d(x)|f(x)} \mu_p d(x) \sum_{i=1}^{p^{deg(f(x))-deg(d(x))}} 1$$

$$= \sum_{d(x)|f(x)} \mu_p(d(x)).\frac{p^{deg(f(x))}}{p^{deg(d(x))}}$$

Therefore $\phi_p(f(x)) = \sum_{d(x)|f(x)} \mu_p(d(x)).\frac{p^{deg(f(x))}}{p^{deg(d(x))}}$

Theorem 2.2.3 For $deg(f(x)) \geq 0$ we have

$\phi_p(f(x)) = p^{deg(f(x))} \prod_{g(x)|f(x)} (1 - \frac{1}{p^{deg(g(x))}})$ where the product runs over the irreducible factors of $f(x)$.

Proof. If $deg(f(x)) = 0$ we have $f(x) = c$ and by definition we have $\phi_p(f(x)) = \phi_p(c) = 1$. On the R.H.S the product is empty and as $p^{deg(f(x))} = p^0 = 1$. Therefore the result holds for $deg(f(x)) = 0$.

Now if $deg(f(x)) > 0$ and let $f(x) = g_1^{e_1}.g_2^{e_2} \ldots g_r^{e_r}$, Then

$$\prod_{g(x)|f(x)} (1 - \frac{1}{p^{deg(g(x))}}) = \prod_{i=1}^{r} (1 - \frac{1}{p^{deg(g_i(x))}})$$

$$= 1 - \sum_i \frac{1}{p^{deg(g_i(x))}} + \sum_{i,j} \frac{1}{p^{deg(g_i(x))}.p^{deg(g_j(x))}} + \ldots + \frac{(-1)^r}{p^{deg(g_1(x))} \ldots . p^{deg(g_r(x))}}$$

$$= 1 - \sum_i \frac{1}{p^{deg(g_i(x))}} + \sum_{i,j} \frac{1}{p^{deg(g_i(x))+deg(g_j(x))}} + \ldots + \frac{(-1)^r}{p^{deg(g_1(x))+..+deg(g_r(x))}}$$

$$= 1 - \sum_i \frac{1}{p^{deg(g_i(x))}} + \sum_{i,j} \frac{(-1)^2}{p^{deg(g_i(x).g_j(x))}} + \ldots + \frac{(-1)^r}{p^{deg(g_1(x)\ldots g_r(x))}}$$

$$= \sum_{d(x)|f(x)} \frac{\mu_p(d)}{p^{deg(d(x))}} \frac{p^{deg(f(x))}}{p^{deg(f(x))}}$$

$$= \frac{1}{p^{deg(f(x))}} \sum_{d(x)|f(x)} \frac{\mu_p(d).p^{deg(f(x))}}{p^{deg(d(x))}}$$

$$= \frac{1}{p^{deg(f(x))}}.\phi_p(f(x))$$

$$\phi_p(f(x)) = p^{deg(f(x))}.\prod_{g(x)|f(x)}(1-\frac{1}{p^{deg(g(x))}})$$

where the product is over $g(x)$, irreducible factors of $f(x)$

Example 2.2.4 Let $f(x) = x^2 + x + 2 \in Z_3[x]$, then $f(x)$ is an irreducible polynomial over Z_3 and $Z_3[x]/(x^2 + x + 2)$ is a field with 3^2 elements, [4] therefore there are $(3^2 - 1) = 8$ invertible elements in this field,that is $\phi_p(f(x)) = 8$.

Now by the above formula we have $\phi_p(f(x)) = p^{deg(f(x))}.\prod_{g(x)|f(x)}(1-\frac{1}{p^{deg(g(x))}})$

$$\phi_3(x^2 + x + 2)) = 3^2.(1-\frac{1}{3^2})$$

$$= 3^2 - 1$$

$$= 8.$$

The group of units is given as

$\{g(x) \in Z_3/(f(x)) : g(x) = ax + b; a, b \in Z_3 \text{ and } (g(x), f(x)) = 1\}$

Example 2.2.5*Let* $f(x) = x^2 + 2$ *and* $Z_3[x]$, then $f(x) = x^2 + 2$ is reducible over Z_3 and

$f(x) = x^2 + 2 = (x-1)(x+1)$.

Now by the above formula we have

$$\phi_p(f(x)) = p^{deg(f(x))}.\prod_{g(x)|f(x)}(1-\frac{1}{p^{deg(g(x))}})$$

$$= 3^2(1-\frac{1}{3})(1-\frac{1}{3})$$

$$= (3-1)(3-1)$$

$$= 2.2$$

$$= 4$$

Further given $f(x) = x^2 + 2 \in Z_3[x]$, $\phi_3(f(x)) = 4$ and note that $\{0,1,2,x,x+1,x+2,2x,2x+1,2x+2\}$ is the set of all elements of $Z_3[x]/(x^2+2)$ and the four invertible elements are $\{1,2,x,2x\}$.

3 Conclusion:

The 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* Springer-Verlag, New York Inc.

[2] P.B.Battacharya, S.K.Jain and S.R.Nagpaul, *BASIC ABSTRACT ALGEBRA*, Second Edition, 1995, cambridge university press,ISBN 0-521-46629-6.

[3] Alina Carmen Cojocaru and M.RamMurty, *An Introduction to Sieve Methods and their Applications*, cambridge university press,2005,ISBN-13 978-0-521-17034-5.

[4] ABHIJIT DAS, *Computational Number Theory*, CRC Press,A CHAPMAN and HALL BOOK.

[5] Kenneth Ireland and Michael Rosen, *A Classical Introduction to Modern Number Theory*, 1972, Spring Science+Business Media LLC, ISBN 978-1-4757-17815.

[6] David M.Burton, *Elementary Number Theory*, Universal Bookstall.

[7] Victor Shoup, *A computational Introduction to Number Theory and Algebra*, 2005, cambridge university press,ISBN-13 978-0-521-85154-1

[8] Gary L.Muller, Carl Mummert,*Finite Fields and Appilications*, Indian Edition, STUDENT MATHEMATICAL LIBRARY, Volume 41, ISBN 9780821887325

[9] James. J.Tattersall, *Elementary Number Theory in Nine Chapters*, second Edition, cambridge university press, ISBN 978-1-107-67000-6.

[10] Rudolflidl and Harald Niederreiter, *Finite Fields*, cambridge university press, ISBN 0521392314.

[11] S.R.Nagpaul, S.K.Jain, textitTopics in applied Abstract Algebra, Indian Edition, American Mathematical Society, ISBN 978-0-8218-5213-2.