IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-0661, p-ISSN: 2278-8727, Volume 17, Issue 2, Ser. 1 (Mar. – Apr. 2021), PP 67-69
www.iosrjournals.org

Factorization of some Polynomials X^n - 1 over GF(q) / < p(x)>

Kulvir Singh
Department of Mathematics, Government College, Bhiwani (India)

Abstract: *Let $g.c.d.(n,p)=1$, where, n be a positive integer and p be a prime. Whenever a finite field of order p^m is required then certainly we are in need of some prime polynomial of degree m over GF(p). Here we study the problem of factorization of x^n-1 as a product of irreducible polynomials. Factorization of x^5-1 over $GF(2)$ and factorization of x^7-1, x^{40} - 1 & x^{80}-1 over $GF(3)$ are obtained through cyclotomic cosets.*

Keywords: *Cyclotomic Coset , Cyclotomic Polynomial, Irreducible polynomial, primitive element.*

Date of Submission: 10-03-2021 Date of Acceptance: 30-03-2021

I. Introduction

Let n≥1 be a positive integer and p is a prime number s.t. (p,n)= 1. If F is a finite field then o(F)=p^n [2] . Consider GF(q), where q is some prime power of p. Then (q,n)=1. To obtain factorization of x^n-1 over GF(q) , we define cyclotomic classes and partition the set S={0,1,2,…,n-1} of integers into cyclotomic classes modulo n over GF(q). Since g.c.d.(n,q)=1, there exist a smallest positive integer 'm' s.t. $q^m \equiv 1$ (mod m) {by Euler Fermat Theorem and also m= $\phi\ (n)$ } [1]. This m is called multiplicative order of q modulo n. In S define a relation '~' as follows. For a, b ∈ S, say that a ~ b if a ≡ bq^i(mod n) for some positive integer 'i'. This relation is an equivalence relation. This relation partition S into equivalence classes. Each equivalence class is called q-cyclotomic class or coset mod n. The q-cyclotomic coset which contain s ∈ S will be C_s={s,qs,…,($q^m{}_s$ -1}s}, where m_s be the least positive integer such that s ≡ $q^m{}_s$ .s (mod n) [by 4]. Also by by [5],

We observe that x^n-1= $\prod_{\substack{d/n \\ 1\le d\le n}} \phi_d(x)$, where $\phi_d(x)$ is the nth cyclotomic polynomials. If C_s is the cyclotomic coset, (mod n) over GF(p), containing the integer s, then, $\prod_{i\in C_s}(x-\alpha^i)$ is the minimal polynomial of α^s over GF(p) [21]. Observe that irreducible polynomials of degree n over $GF(p\ )$, help us in the construction of finite field $GF(p^n)$. Construction of some finite field GF(3^3) & GF(3^4) over GF(3) are studied by Singh K.[3]. If x^q - x =f(x).g(x), then every element in the field must be a root of f(x) or g(x). The case f(x) = x, g(x) = x^{q-1} - x separate the zero elements from the non zero elements. To separate the non zero elements according to their order , a factorization of the polynomial x^{q-1}- x is needed. Further, whenever a finite field of order p^m is required then certainly we are in need of some prime polynomial of degree m over GF(p). The above facts basically highlight the utility of factor of polynomial x^n-1. Then how to find out these factors , is the basic aim of this paper.

Notations 1.1: (i) $M_i(x)$ represents minimal polynomials
(ii) C_s denote q-cyclotomic class containing s∈ S.
(iii) $\phi_n(x)$ represents the nth cyclotomic polynomial.
(iv) $\phi(x)$ denote the Euler's totient function.

Definition 1.2:
(i) Euler totient function: The Euler totient function $\phi(n)$ is defined for all integer 'n' s.t. $\phi(n)=1$ for n=1, and $\phi(n)$ represent the number of positive integer less than 'n' and co- prime to 'n'.
(ii) Cyclotomic polynomial: Let S be the set of all primitive nth root of unity , then
$\phi_n(x)=\prod_{\lambda\in s}(x-\lambda)$ is called nth cyclotomic polynomial.

II. Algorithm For Factorizing The Polynomials Of The Type X^n -1 Over Some Finite Field

Step. 1. Find multiplicative order of q mod n.
2. Choose an irreducible polynomial of degree m over GF(q) and denote it by p(x).
3. Find F= GF(q)/< p(x)>, which is a field of order q^m.
4. Find a primitive element of field F.
5. Find out primitive nth root of unity.
6. Find cyclotomic classes mod n over GF(q).
7. Find minimal polynomials $M_s(x)$ of α^S which will be $\prod_{i\in C_s}(x-\alpha^i); s\in S$.

8. Calculate x^n-1 = $\prod_s M_s(x)$; where s runs over a set of representative of cyclotomic cosets.

III. Factorization Of Polynomial X^n-1 Over GF(Q)

(Particular case for n=5 & q=3 ; n=7 & q=3 ; n=40 & q=3 ; n=80 & q=3)

3.1. Consider $X^5 – 1$ over GF(3)

The smallest natural number m s.t. $5/(3^m-1)$ is 4 and choose an irreducible polynomial polynomial of degree 4 over GF(3). Here p(x)= X^4+x^2+x+1. Is an irreducible polynomial of degree 4.
Hence, GF(3)[x]/< x^4+x^2+x+1> is a field of order 3^4=81.
Take I= < x^4+x^2+x+1> . Consider $\alpha=x^2+1+< x^4+x^2+x+1>$ i.e. $\alpha = x^2+1+I \in F$.
This α is a primitive element of F. Taking $\beta= \alpha^{16}$, β will be a primitive 5^{th} root of unity. Now 3-cyclotomic cosets mod(5) are
$C_0=\{0\}$, $C_1=\{1,3,4,2\}$
Corresponding minimal polynomials are
$M_0(X)= (X- \beta^0)= X-1$
$M_1(X)=(X - \beta) (X - \beta^2)(X - \beta^3)(X - \beta^4) = X^4 - X^3 (\beta^4+ \beta^3 + \beta^2+ \beta)+X^2(\beta^7+ \beta^6+2\beta^5+ \beta^3) +x(\beta^9+ \beta^8 + \beta^7+ \beta^6)+ \beta^{11}$
Now to find β^2, β^3 , β^4 and so on we start as follows
Since $\alpha^4+ \alpha^3=1$ i.e. $\alpha^4 = -\alpha^3+1$ i.e. $\alpha^5 = -\alpha^4+ \alpha= \alpha^3+\alpha+1$
$\alpha^6= -\alpha^6+ \alpha^2- \alpha+1$ i.e. $\alpha^8 = \alpha^2- \alpha-1$
$\beta= \alpha^{16} = -\alpha^2- \alpha-1$ i.e. $\beta^2 = \alpha^3- \alpha-1$
$\beta^3 = -\alpha^2+ \alpha+1$ $\beta^4 = -\alpha^3- \alpha^2 + \alpha$
$\beta^{5=} \beta^3 \beta^2 = \alpha^5- \alpha^4+ \alpha^3 - \alpha =1$
$\beta^{6=} \beta$, $\beta^{7=} \beta^2$, $\beta^{8=} \beta^3$, $\beta^{9=} \beta^4$
$\beta=x^2 -2x+1$, $\beta^2 = -x^3 -x^2+x$
$\beta^3= x+2=x-1$, $\beta^4 = x^3-1$, $\beta^5 = 1$
Now, $M_1(X)=x^4+ x^3-2 x^2+x+1$
$X^5 – 1= M_0(X)M_1(X)= (x-1)(x^4+ x^3-2 x^2+x+1)$

3.2. Consider $x^7 – 1$ over GF(2)

Here multiplicative order of 3 mod(40) is 4.
$p(x)=x^4+x+2$ is an irreducible polynomial of degree 4.
Hence, GF(2)[x]/<x^3+x+2> is a field of order 2^3=8.
Take I= <x^3+x+1>. Consider $\alpha=x+I \in F$.
This α is a primitive element of F. Also α will be a primitive 7^{th} root of unity. Now 2-cyclotomic cosets mod(7) are
$C_0=\{0\}$, $C_1=\{1,2,4\}$, $C_3=\{3,6,5\}$,
Corresponding minimal polynomials are
$M_0(X)= (x- \alpha^0)= x-1$
$M_1(X)= (x - \alpha) (x - \alpha^2) (x - \alpha^4) = x^4 - x^3 + x^2 +1$
$M_2(X)= (x – \beta^2) (x – \beta^6) (x – \beta^{18}) (x – \beta^{14}) = x^3 – x^2 - 1$
Hence,
$x^7 - 1= (x-1)(x^3 + x -1) (x^3 – x^2- 1)$.

3.3. Consider $x^{40} – 1$ over GF(3)

Here multiplicative order of 3 mod(40) is 4.
$p(x)=x^4+x+2$ is an irreducible polynomial of degree 4.
Hence, GF(3)[x]/<x^4+x+2> is a field of order 3^4=81.

Take I= $<x^4+x+2>$. Consider $\alpha=x^3+1+I= x^3+1 \in F$.
This α is a primitive element of F. Then $\beta= \alpha^2$ and α will be a primitive 40^{th} root of unity. Now 3-cyclotomic cosets mod(40) are
$C_0=\{0\}$, $C_1=\{1,3,9,27\}$, $C_2=\{2,6,18,14\}$, $C_4=\{4,12,36,28\}$, $C_5=\{5,15\}$, $C_7=\{7,21,23,29\}$, $C_8=\{8,24,32,16\}$, $C_{10}=\{10,30\}$, $C_{11}=\{11,33,19,17\}$, $C_{13}=\{13,39,37,31\}$, $C_{20}=\{20\}$, $C_{25}=\{25,35\}$, $C_{26}=\{26,38,34,22\}$.
Corresponding minimal polynomials are
$M_0(x)= (x- \beta^0)= x-1$
$M_1(x)= (x - \beta) (x - \beta^3) (x - \beta^9) (x - \beta^{27}) = x^4 - x^3 + x^2 +1$
$M_2(x)= (x – \beta^2) (x – \beta^6) (x – \beta^{18}) (x – \beta^{14}) = x^4 + x^3 - x+1$
$M_4(x)= x^4 - x^3 + x^2 - x+1$ $M_5(x)= x^2 – x – 1$
$M_7(x)= x^4 + x^3 + x^2 + 1$ $M_8(x)= x^4 + x^3 + x^2 + x+1$ $M_{10}(x)= x^2 – x+1$
$M_{11}(x)= x^4 + x^2 + x+1$
$M_{13}(x)= x^4 +x^2- x+ 1$ $M_{20}(x)= x+1$ $M_{25}(x)= x^2 + x-1$
$M_{26}(x)= x^4 - x^3 + x+1$
Hence,
$x^{40} - 1= (x-1)(x^4 - x^3 + x^2 +1) (x^4 + x^3 - x+1)(x^4 - x^3 + x^2 - x+1) (x^2 – x – 1)$
$(x^4 + x^3 + x^2 + 1) (x^4 + x^3 + x^2 + x+1) (x^2 – x+1) (x^4 + x^2 + x+1) (x^4 +x^2- x+ 1) (x+1) (x^2 + x-1)(x^4 - x^3 + x+1)$.

3.4. Consider X^{80} – 1 over GF(3)
Here multiplicative order of 3 mod(80) is 4.
$p(x)=x^4+x+2$ is an irreducible polynomial of degree 4.
Hence, $GF(3)[x]/<x^4+x+2>$ is a field of order $3^4=81$.
Take I= $<x^4+x+2>$. Consider $\alpha=x^3+1+I= x^3+1 \in F$.
This α is a primitive element of F and αwill be a primitive 80^{th} root of unity. Now 3-cyclotomic cosets mod(80) are
$C_0=\{0\}$, $C_1=\{1,3,9,27\}$, $C_2=\{2,6,18,54\}$, $C_4=\{4,12,36,28\}$, $C_5=\{5,15,45,55\}$, $C_7=\{7,21,63,29\}$, $C_8=\{8,24,72,56\}$, $C_{10}=\{10,30\}$, $C_{11}=\{11,33,19,57\}$, $C_{13}=\{13,39,37,31\}$,$C_{14}=\{14,42,46,58\}$, $C_{16}=\{16,48,64,32\}$, $C_{17}=\{17,51,73,59\}$, $C_{20}=\{20,60\}$, $C_{22}=\{22,66,38,34\}$, $C_{23}=\{23,69,47,61\}$, $C_{25}=\{25,75,65,35\}$, $C_{26}=\{26,78,74,62\}$, $C_{40}=\{30\}$, $C_{41}=\{41,43,49,67\}$, $C_{44}=\{52,76,68,44\}$, $C_{50}=\{50,70\}$, $C_{53}=\{53,79,77,71\}$.
Now minimal polynomials are
$M_0(x)= (x - \alpha^0)= x-1$
$M_1(x)= (x - \alpha) (x - \alpha^3) (x - \alpha^9) (x - \alpha^{27}) = x^4 - x^3 – 1$
$M_2(x)= (x – \alpha^2) (x – \alpha^6) (x – \alpha^{18}) (x – \alpha^{54}) = x^4 - x^3 + x^2+1$
$M_4(x)= (x – \alpha^4) (x – \alpha^{12}) (x – \alpha^{36}) (x – \alpha^{28}) = x^4 + x^3 – x +1$
$M_5(x)= (x – \alpha^5) (x – \alpha^{15}) (x – \alpha^{45}) (x – \alpha^{55}) = x^4 – x^2 – 1$
$M_7(x)= (x – \alpha^7) (x – \alpha^{21}) (x – \alpha^{63}) (x – \alpha^{29}) = x^4 + x^3 – x^2 + x-1$
$M_8(x)= x^4 - x^3 + x^2 – x+1$ $M_{10}(x)= x^2 – x+1$
$M_{11}(x)= x^4 - x^3 + x^2 + x-1$ $M_{13}(x)= x^4 - x -1$
$M_{14}(x)= x^4 + x^3 + x^2 +1$ $M_{16}(x)= x^4 - x^3 + x^2 + x+1$
$M_{17}(x)= x^4 + x^3 - x^2 – x-1$ $M_{20}(x)= x^2 –1$
$M_{22}(x)= x^4 + x^2 + x+1$ $M_{23}(x)= x^4 - x^3 - x^2 –x - 1$
$M_{25}(x)= x^4 + x^2 – x +1$ $M_{26}(x)= x^4 + x^2 – x+1$
$M_{40}(x)= x+1$ $M_{41}(x)= x^4 + x^3 -1$
$M_{44}(x)= x^4 - x^3 + x+1$ $M_{50}(x)= x^2 + x-1$
$M_{53}(x)= x^4 + x-1$. Hence,
$x^{80} - 1= (x-1)(x^4 -x^3 –1)(x^4 - x^3 + x^2+1)(x^4 + x^3 - x+1) (x^4 – x^2 – 1) (x^4 +x^3 –x^2 + x-1)$
$(x^4 - x^3 + x^2 – x+1)(x^2 – x+1)(x^4 - x^3 + x^2 + x-1) (x^4 - x-1) (x^4 + x^3 + x^2 +1) (x^4 - x^3 + x^2 + x+1) (x^4 + x^3 - x^2 – x-1)(x^2 –1)(x^4 + x^2 + x+1)(x^4 - x^3 - x^2 –x - 1)(x^4 + x^2 – x+1) (x^4 + x^2 – x+1) (x+1)(x^4 + x^3 -1)(x^4 - x^3 + x+1)(x^2 + x-1)(x^4 + x-1)$.

References

[1]. Herstein, I N (1976), Topics in Algebra, Vikas Publishing House, New Delhi.
[2]. Khanna, Vijay K and Bhambri, S K. (1993), A Course in Abstract Algebra, Vikas Publishing House New Delhi.
[3]. Singh Kulvir (IJMSI) E-ISSN: 2321 – 4767 P-ISSN: 2321 - 4759 Volume 1 Issue 1 ǁ August. 2013ǁ PP-44-47.
[4]. Vermani L.R. (1964), Elements of Algebraic Coding Theory, CHAPMAN & HALL, MATHEMATICS.
[5]. Zameerudin Quazi and Surjeet Singh (1975), Modern Algebra, Vikas Publishing House New Delhi.