IOSR Journal of Mathematics (IOSR-JM)
e-ISSN: 2278-5728, p-ISSN: 2319-765X. Volume 17, Issue 4 Ser. I (Jul. – Aug. 2021), PP 58-67
www.iosrjournals.org

Factorization of some Polynomials over GF(q) / < p(x)> - II

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

Abstract: *Let Let F=GF(q) be a field of q elements and f(x) =* $\sum_{k=0}^{m} g_i x^i$ *a monic polynomial of degree m over F .*

Let Q = $Q_{i,j}$ *be a square matrix over F in which ith row is represented by* $x^{q(i-1)}$ *reduced modulo f(x). Here we factorized polynomial of type* x^n *- 1 with the help of Berlekamp's algorithm over the finite field F. Factorization of* $x^{10} + 1$, $x^{20} + 1$, $x^{20} – 1$ *&* $x^{40} – 1$ *over GF(3) are obtained.*

Keywords: *Cyclotomic Coset, Monic Polynomial, Finite Field, Multiplicative Order.*

I. Introduction

In the construction of finite fields, we were required to find certain irreducible factors of $x^n – 1$ where n= $p^m – 1$, p a prime. Let p be a prime, n a positive integer not divisible by p and q is a power of p. If F is a finite field then by [3], o(F) = p^n. 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) [2]. 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) [6]. Also we know 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 [7]. If C_s is the cyclotomic coset, (mod n) over GF(p), containing the integer s, then, by [6], $\prod_{i \in C_s} (x - \alpha^i)$ is the minimal polynomial of α^s over GF(p). 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.[4]. 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 main problem. 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 by Singh K. [5] through cyclotomic cosets.

The Berlikamp's algorithm for the factorization of the polynomials f(x) over finite field is described in this paper. The algorithm is then applied to factorize $x^n - 1$ over GF(q). In the end of paper merits and demerits over the factorization by cyclotomic cosets and with the help of Berlikamp's algorithm are discussed.

II. [1] Berlikamp's Algorithm (General Case) for factorizing the polynomials

Step. 1. Write given polynomial f(x) of degree m over GF(q).

2. Write $[Q_{ij}]_{m\times m}$ in which the ith row is represented by $x^{q(i-1)}$ reduced modulo f(x) i.e. $x^{qi} \equiv \sum_{k=0}^{m-1} Q_{I+1,K+1} x^k \bmod f(x)$; $1 \le i \le m-1$

i.e. $x^{qi} \equiv (Q_{i+1,1}.1+ Q_{i+1,2}.x + Q_{i+1,3}.x^2+\ldots+ Q_{i+1,m}.x^{m-1}) \bmod f(x)$

i.e. $1 \equiv (Q_{11}+ Q_{12}x + Q_{13}x^2+\ldots+ Q_{1m}x^{m-1}) \bmod f(x)$

$x^q \equiv (Q_{21}+ Q_{22}x + Q_{23}x^2+\ldots+ Q_{2m}x^{m-1}) \bmod f(x)$

$x^{2q} \equiv (Q_{31}+ Q_{32}x + Q_{33}x^2+\ldots+ Q_{3m}x^{m-1}) \bmod f(x)$

:

$x^{q(m-1)} \equiv (Q_{m1}+ Q_{m2}x + Q_{33}x^2+\ldots+ Q_{mm}x^{m-1}) \bmod f(x)$

Then,

$$Q = \begin{bmatrix} Q_{11} & Q_{12} & \cdots & Q_{1m} \\ Q_{21} & Q_{22} & \cdots & Q_{2m} \\ : & : & \ldots & : \\ Q_{m1} & Q_{m2} & \cdots & Q_{mm} \end{bmatrix}$$

3. Take g(x)= $\sum_{k=0}^{m-1} g_i x^i$, any general polynomial of degree m-1.

Find $g_0, g_1, g_2, \ldots g_{m-1}$ s.t. $(g_0, g_1, g_2, \ldots. g_{m-1})(Q-I)= O$

4. Find $\prod_{s\in F} g.c.d.(f(x), g(x)-s) = 0$, which will be factorization of f(x).

Example. 2.1. Let $f(x) = 1+x + x^2 + x^6 +x^7+x^8+x^{12}$

i.e. f(x) = 111 000 111 0001

Here F= {0,1}= GF(2)

For matrix $Q_{12\times 12}$ we need $x^{2(i-1)} \equiv (-) (\bmod f(x))$; $1 \le i \le 12$

i.e. $1 \equiv 1 \pmod{f(x)}$, $x^2 \equiv x^2 \pmod{f(x)}$, $x^4 \equiv x^4 \pmod{f(x)}$,…,

$x^{20} \equiv (1+ x+ x^4 + x^7 +x^8 +x^9) \pmod{f(x)}$,

$x^{22} \equiv (x^2+ x^3 + x^6 +x^9 +x^{10} +x^{11}) \pmod{f(x)}$

We can write

1 = 100000000000, x = 010000000000, x^2 = 001000000000

x^4 = 000010000000, x^6 = 000000100000, x^8 = 000000001000

x^{10} = 000000000010, x^{12} = 111000111000, x^{14} = 001110001110

x^{16} = 111011011011, x^{18} = 101010010010, x^{20} = 110010011100

x^{22} = 001100100111

Hence,

$$Q=\begin{bmatrix}1&0&0&0&0&0&0&0&0&0&0&0\\0&0&1&0&0&0&0&0&0&0&0&0\\0&0&0&0&1&0&0&0&0&0&0&0\\0&0&0&0&0&0&1&0&0&0&0&0\\0&0&0&0&0&0&0&0&1&0&0&0\\0&0&0&0&0&0&0&0&0&0&1&0\\1&1&1&0&0&0&1&1&1&0&0&0\\0&0&1&1&1&0&0&0&1&1&1&0\\1&1&1&0&1&1&0&1&1&0&1&1\\1&0&1&0&1&0&0&1&0&0&1&0\\1&1&0&0&1&0&0&1&1&1&0&0\\0&0&1&1&0&0&1&0&0&1&1&1\end{bmatrix}\qquad Q-I=\begin{bmatrix}0&0&0&0&0&0&0&0&0&0&0&0\\0&1&1&0&0&0&0&0&0&0&0&0\\0&0&1&0&1&0&0&0&0&0&0&0\\0&0&0&1&0&0&1&0&0&0&0&0\\0&0&0&0&1&0&0&0&1&0&0&0\\0&0&0&0&0&1&0&0&0&0&1&0\\1&1&1&0&0&0&0&1&1&0&0&0\\0&0&1&1&1&0&0&1&1&1&1&0\\1&1&1&0&1&1&0&1&0&0&1&1\\1&0&1&0&1&0&0&1&0&1&1&0\\1&1&0&0&1&0&0&1&1&1&1&0\\0&0&1&1&0&0&1&0&0&1&1&0\end{bmatrix}$$

Operate $C_7 \rightarrow C_7 + C_4$; $C_9 \rightarrow C_2 + C_3 + C_5 + C_9$; $C_{11} \rightarrow C_{11} + C_6$ on $Q-I$, we obtain,

$$Q-I=\begin{bmatrix}0&0&0&0&0&0&0&0&0&0&0&0\\0&1&1&0&0&0&0&0&0&0&0&0\\0&0&1&0&1&0&0&0&0&0&0&0\\0&0&0&1&0&0&0&0&0&0&0&0\\0&0&0&0&1&0&0&0&0&0&0&0\\0&0&0&0&0&1&0&0&0&0&0&0\\1&1&1&0&0&0&0&1&1&0&0&0\\0&0&1&1&1&0&1&1&1&1&1&0\\1&1&1&0&1&1&0&1&1&0&0&1\\1&0&1&0&1&0&0&1&0&1&1&0\\1&1&0&0&1&0&0&1&1&1&1&0\\0&0&1&1&0&0&0&0&1&1&1&0\end{bmatrix}$$

Now let, $g(x) = g_0 + g_1x + g_2x^2 + ... + g_{11}x^{11}$ be a polynomial of degree 11

To find coefficient of polynomial g(x), we have

$$\left[g_{0,}\,g_1,g_{2,}\ldots,g_{11}\right].\begin{bmatrix}0&0&0&0&0&0&0&0&0&0&0&0\\0&1&1&0&0&0&0&0&0&0&0&0\\0&0&1&0&1&0&0&0&0&0&0&0\\0&0&0&1&0&0&0&0&0&0&0&0\\0&0&0&0&1&0&0&0&0&0&0&0\\0&0&0&0&0&1&0&0&0&0&0&0\\1&1&1&0&0&0&0&1&1&0&0&0\\0&0&1&1&1&0&1&1&1&1&1&0\\1&1&1&0&1&1&0&1&1&0&0&1\\1&0&1&0&1&0&0&1&0&1&1&0\\1&1&0&0&1&0&0&1&1&1&1&0\\0&0&1&1&0&0&0&0&1&1&1&0\end{bmatrix}=O$$

Which gives, $g_2 = g_5 = g_7 = g_8 = g_{10} = 0$ and $g_1 = g_9 = g_{11}$; $g_3 = g_4 = g_6$

Hence, $g(x) = g_0 + g_1x + g_3x^3 + g_4x^4 + g_6x^6 + g_9x^9 + g_{11}x^{11}$

i.e. $g(x) = B + Ax + Ax^3 + Ax^4 + Ax^6 + Ax^9 + Ax^{11}$; where A,B ∈ GF(2) .

Take A=1 and B is arbitrary. Now we shall find the g.c.d. of (f(x), g(x)) and (f(x), g(x)-I), we have

(f(x), g(x)) = 10011101 and (f(x), g(x)-I) = 111101. Hence,

$f(x) = (100111010)(\ 111101) = (1+ x^3 + x^4 + x^5+x^7)(\ 1+x + x^2 + x^3+x^5\ )$

Example 2.2 Let $f(x) = x^5 + 1$ over GF(3)

The successive power of x needed for Q- matrix obtained by taking $x^{3(i-1)}$ modulo f(x) for $1 \le i \le 5$ are 1, x^3, x^6, x^9, x^{12}

Hence

$$Q=\begin{bmatrix}1&0&0&0&0\\0&0&0&1&0\\0&-1&0&0&1\\0&0&0&0&-1\\0&0&1&0&0\end{bmatrix}\qquad Q-I=\begin{bmatrix}0&0&0&0&0\\0&-1&0&1&0\\0&-1&-1&0&1\\0&0&0&-1&-1\\0&0&1&0&-1\end{bmatrix}$$

Now let, $g(x) = g_0 + g_1x + g_2x^2 + g_3x^3+ g_4x^4$ s.t. $(g_0, g_1, g_2, g_3, g_4)(Q - I) = O$, we obtain $g_1 = - g_2 = g_3 = - g_4$ and g_0 is any arbitrary element of GF(3). Take $g_0 = g_1=g_3 = 1$ & $g_2 = g_4 = - 1$. Now find out g.c.d. (f(x) , g(x)-s) ; s ∈ GF(3)

For s = 0, (f(x) , g(x)-s) = x- 2

s = 1, (f(x) , g(x)-s) = 1

s = 2, (f(x) , g(x)-s) = $x^4 + 2x^3 + x^2 + 2x + 1$

$\Rightarrow$ $x^5 + 1 = (x+1)(x^4 + 2x^3 + x^2 + 2x + 1)$

Example 2.3 Let f(x) = $x^{10} + 1$ over GF(3)

The successive power of x needed for Q- matrix obtained by taking $x^{3(i-1)}$ modulo f(x) for $1 \le i \le 10$ are 1, x^3, x^6, x^9, x^{15}, x^{18}, x^{21}, x^{24}, x^{27}

$$Q = \begin{bmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \end{bmatrix}$$

$$Q - I = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & -1 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & -1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & -1 & 0 & -1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & -2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & -1 & 0 \\ 0 & 1 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & -1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & -1 \end{bmatrix}$$

Let g(x)= $\sum_{k=0}^{9} g_i x^i$ s.t. $(g_0, g_1, g_2, \ldots, g_8, g_9)(Q - I) = O$ i.e.

$g_1 = g_3 = g_7$; $g_2 = -g_4 = g_6 = -g_8 = g_9$ and $g_5=0$. Taking

$g_0 = g_1 = g_3 = g_7 = g_6 = g_2 = g_9 = 1$; $g_4 = g_8 = -1$ and $g_5 = 0$

$\Rightarrow$ g(x) = $1+x +x^2 +x^3 - x^4 +x^6 +x^7 - x^8 +x^9$

Now find out g.c.d. (f(x) , g(x)-s) ; s ∈ GF(3)

For s = 0, (f(x) , g(x)-s) = $x^6 + 2x^5 + x^4 + x^2 +x + 1$

s = 1, (f(x) , g(x)-s) = $x^4 + x^3 - x + 1$

s = 2, (f(x) , g(x)-s) = 1

$\Rightarrow$ $x^{10} + 1 = (x^6 + 2x^5 + x^4 + x^2 + x + 1)(x^4 + x^3 - x + 1)$

Example 2.4. Let f(x) = $x^{20} + 1$ over GF(3)

The successive power of x needed for Q- matrix obtained by taking $x^{3(i-1)}$ modulo f(x) for $1 \leq i \leq 20$ are 1, x^3, x^6, x^9, x^{12}, x^{15}, x^{18}, x^{21}, x^{24}, x^{27}, x^{30}, x^{33}, x^{36}, x^{39}, x^{42}, x^{43}, x^{48}, x^{51}, x^{54}, x^{57}

$$Q = \begin{bmatrix}
1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & -1 \\
0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0
\end{bmatrix}$$

$$Q-I=\begin{bmatrix}
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&-1&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&-1&0&0&0&1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&-1&0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&-1&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0\\
0&0&0&0&0&-1&0&0&0&0&0&0&0&0&0&1&0&0&0&0\\
0&0&0&0&0&0&-1&0&0&0&0&0&0&0&0&0&0&0&0&0\\
0&-1&0&0&0&0&0&-1&0&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&-1&0&-1&0&-1&0&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&-1&0&-1&0&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&-2&0&0&0&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&-1&0&-1&0&0&0&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&-1&0&0&0&-1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&-1&0&0&0&0&0&-1\\
0&0&1&0&0&0&0&0&0&0&0&0&0&0&-1&0&0&0&0&0\\
0&0&0&0&0&1&0&0&0&0&0&0&0&0&0&-1&0&0&0&0\\
0&0&0&0&0&0&0&0&1&0&0&0&0&0&0&0&-1&0&0&0\\
0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&0&0&-1&0&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&0&0&-1&0\\
0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&0&1&0&-1
\end{bmatrix}$$

Let g(x)= $\sum_{k=0}^{19} g_i x^i$ s.t. (g_0, g_1, g_2, …,g_{18}, g_{19})(Q - I) = O i.e.

$\Rightarrow$ $g_1 = g_3 = -\ g_7 = g_9$; $g_2 = g_{14} = g_6 = -g_{18}$; $g_4 = -\ g_8 = -\ g_{12} = -\ g_{16}$; $g_{11} = -\ g_{13} = g_{17} = -g_{19}$; $g_5 = g_{15}$ and $g_{10} = 0$. Taking

$g_0 = g_1 = g_2 = g_3 = g_4 = g_5 = g_6 = g_9 = g_{10} = g_{11} = g_{12} = g_{14} = g_{15} = g_{17} = g_{18} = g_{19} = 1$; $g_7 = g_8 = g_{13} = g_{16} = -1$ and $g_{10} = 0$

$\Rightarrow$ $g(x) = 1+x +x^2 +x^3 + x^4 + x^5 +x^6 - x^7 – x^8 +x^9 + x^{11} +x^{12} – x^{13} + x^{14} +x^{15} – x^{16} + x^{17} +x^{18} + +x^{19}$

Now find out g.c.d. (f(x) , g(x)-s) ; s ∈ GF(3)

For s = 0, (f(x) , g(x) -s) = $x^8 – x^7 + x^6 – x^4 - x^3 +x^2 +1$

s = 1, (f(x) , g(x) -s) = $x^4 + x^2 – x + 1$

s = 2, (f(x) , g(x) -s) = $x^8 + x^7 - x^6 – x^5 + x^4 - x^3 +x +1$

Hence,

$x^{20} + 1 = (x^8 –x^7 + x^6 –x^4 - x^3 +x^2+1)(x^4 + x^2 – x + 1)(x^8 + x^7 - x^6 – x^5 + x^4 - x^3 +x +1)$

III. [1]Berlikamp's Algorithm (Special Case) for factorizing the polynomials x^n-1 over *GF(q)*

Step. 1. Write given polynomial f(x) = x^n -1

2.Write down all cyclotomic classes over mod n and count the number of classes , let these be m.

3. In this step we find out polynomial g(x) which will be g(x)= $a_1 + a_2 + [(x)^{\text{first element of second class}} + (x)^{\text{second element of second class}} +\ldots] + a_3 [\ldots] + a_4 [\ldots] +\ldots$ where a_i ∈ GF(q).

4. Find g.c.d. (f(x), g(x)) by taking different value of a_1, a_2, a_3,…

5. x^n-1 = $\prod g.c.d.(f(x), g(x))$

Example. 3.1 Let f(x) = x^3-1 over GF(2)

The 2-cyclotomic cosets mod 3 are

C_0={0}, C_1={1,2}

Therefore, x^3-1 factors as a product of x-1and one irreducible factor of degree 2. The factor of x^3-1 are among the H.C.F. of x^3-1 with a+b(x+x^2) ; a,b ∈ GF(2).

Take a=b=1 in above and then apply Euclid' s algorithm, we obtain

(x^3-1)÷ (1+x+x^2) = x-1

Hence,

(x^3-1)= (1+x+x^2) (x+1)

Example.3.2 Let f(x) = x^5-1 over GF(3)

The 3-cyclotomic cosets mod 5 are C_0={0}, C_1={1,3,4,2}

Therefore, x^5-1 factors as a product of x-1and one irreducible factor of degree 4. The factor of x^5-1 are among the H.C.F. of x^5-1 with a+b(x+x^2+x^3+x^4); a,b ∈ GF(3).

Take a=b=1 in above and then apply Euclid' s algorithm, we obtain

(x^5-1)÷ (1+x+x^3+x^4) = x-1

Hence,

(x^5 - 1)= (1+ x - 2x^2 + x^3 + x^4) (x - 1)

Example. 3.3. Let f(x) = x^7-1 over GF(2)

The 3-cyclotomic cosets mod 7 are C_0={0}, C_1={1,2,4}, C_3=3,6,5}

Therefore, x^7-1 factors as a product of x-1and two irreducible factor of degree 3. The factor of x^7-1 are among the H.C.F. of x^7-1 with a+b(x+x^2+x^4) + c(x^3+x^5+x^6); a,b ∈ GF(2).

Take a=b=1, c=0 in above and then apply Euclid' s algorithm, we obtain

(x^7-1)÷ (1+x+x^2+x^4) = x^3 - x- 1

$\Rightarrow$ g.c.d.(x^7-1 , 1+x+x^2+x^4) = 1+x+x^2+x^4

But we know that x^7 - 1 has two irreducible factor of degree 3 each.

$\Rightarrow$1+x+x^2+x^4 will be reducible and one factor will be x-1 , other factor will be found by actual division i.e,

(1+x+x^2+x^4) ÷ (x – 1) = x^3 +x^2+1

Hence,

(x^7 - 1)= (x^3 +x^2+1) (x^3 – x - 1) (x - 1)

Example. 3.4. Let f(x) = x^{10} - 1 over GF(3)

Here f(x) = x^{10} - 1 = (x^5 – 1) (x^5 + 1)

Note that as in above Example 3.2

(x^5 - 1)= (1+ x - 2x^2 + x^3 + x^4) (x - 1) and by Example 2.2

$(x^5 + 1) = (x - 2)(x^4 + 2x^3 + x^2 + 2x + 1)$

$\Rightarrow x^{10} - 1 = (x - 1)(x - 2)(1 + 2x + x^2 + 2x^3 + x^4)(1 + x + x^2 + x^3 + x^4)$

Example. 3.5 Let $f(x) = x^{20} - 1$ over GF(3)

Now $x^{20} - 1 = (x^{10} - 1)(x^{10} + 1)$

Note that as in above Example 3.4

$x^{10} - 1 = (x - 1)(x - 2)(1 + 2x + x^2 + 2x^3 + x^4)(1 + x + x^2 + x^3 + x^4)$

and by Example 2.3

$(x^{10} + 1) = (1 - x + x^3 + x^4)(1 + x + x^2 + x^4 + 2x^5 + x^6)$

$\Rightarrow x^{20} - 1 = (x - 1)(x - 2)(1 + 2x + x^2 + 2x^3 + x^4)(1 + x + x^2 + x^3 + x^4)$

$(1 - x + x^3 + x^4)(1 + x + x^2 + x^4 + 2x^5 + x^6)$

Example. 3.6 Let $f(x) = x^{40} - 1$ over GF(3)

Now $x^{40} - 1 = (x^{20} - 1)(x^{20} + 1)$

Note that as in above Example 3.5

$x^{20} - 1 = (x - 1)(x - 2)(1 + 2x + x^2 + 2x^3 + x^4)(1 + x + x^2 + x^3 + x^4)$

$(1 - x + x^3 + x^4)(1 + x + x^2 + x^4 + 2x^5 + x^6)$

and by Example 2.4

$(x^{20} + 1) = (1 + x^2 - x^3 - x^4 + x^6 - x^7 + x^8)(1 - x + x^2 + x^4)(1 + x - x^2 - x^3 + x^4 - x^5 - x^6 + x^7 + x^8)$

$\Rightarrow x^{40} - 1 = (x - 1)(x - 2)(1 + 2x + x^2 + 2x^3 + x^4)(1 + x + x^2 + x^3 + x^4)$

$(1 - x + x^3 + x^4)(1 + x + x^2 + x^4 + 2x^5 + x^6)(1 + x^2 - x^3 - x^4 + x^6 - x^7 + x^8)(1 - x + x^2 + x^4)(1 + x - x^2 - x^3 + x^4 - x^5 - x^6 + x^7 + x^8)$

Also we have

$x^6 + 2x^5 + x^4 + x^2 + x + 1 = (x^2 + 1)(x^4 - x^3 + x + 1)$

$x^8 - x^7 + x^6 - x^4 - x^3 + x^2 + 1 = (x^4 - x^3 + x^2 + 1)(x^2 - x + 1)(x^2 + x - 1)$

$x^8 + x^7 - x^6 - x^5 + x^4 - x^3 - x^2 + x + 1 = (x^4 + x^3 + x^2 + 1)(x^4 + x^2 + x + 1)$

Hence

$x^{40} - 1 = (x - 1)(x - 2)(1 + 2x + x^2 + 2x^3 + x^4)(1 + x + x^2 + x^3 + x^4)$

$(1 - x + x^3 + x^4)(1 - x + x^2 + x^4)(x^2 + 1)(x^4 - x^3 + x + 1)(x^4 - x^3 + x^2 + 1)(x^2 - x + 1)(x^2 + x - 1)(x^4 + x^3 + x^2 + 1)(x^4 + x^2 + x + 1)$

IV. Comparison between the two methods(i.e. factorization through cyclotomic coset and factorization with the help of Berlikamp's algorithm) :-

Method I : (Factorization Through Cyclotomic Cosets)

(i) This method is useful for finding the irreducible factors of the polynomial $x^n - 1$ over GF(q) where $(n, q) = 1$.

(ii) For large 'n' the number of cyclotomic cosets may be large.

(iii) If ‘m’ the multiplicative order of q mod n, is large then some times it is difficult to find a irreducible polynomial of degree m.

(iv) For large q it is difficult to find primitive element of GF(q).

(v) If the size of a cyclotomic cosets is large, then to find corresponding minimal polynomial is difficult.

(vi) For large ‘n’ it is again difficult to find primitive nth root of unity.

(vii) The number of cyclotomic cosets and their size respectively gives information regarding the number of irreducible factors of $x^n - 1$ and their degree.

Basically this method is very appropriate for factorizing $x^n - 1$ for small ‘n’ over GF(q), where ‘m’ is also small.

Method II : (Factorization Through Berlikamp,s Algorithm)

(i) This method is helpful for finding the factors of a general polynomial of degree m over GF(q).

(ii) For large m, the Q-matrix becomes very large.

(iii) In general case, to find the coefficient of the polynomial g(x) s.t. g(x).[Q – I] = O is laborious.

(iv) If q is large, then it is difficult to find g.c.d.(f(x), g(x) – s), where s ∈ GF(q).

(v) The factor of f(x) may not be irreducible.

(vi) In general case, we have many choice for the coefficient of g(x). We can choose those coefficient which reduces the calculation work.

(vii) In special case , if ‘n’ is large then the number of cyclotomic cosets may be large.

(viii) In special case, if number of cyclotomic cosets is large or the size of the cyclotomic coset is large, then to find g(x) is difficult.

V. Conclusion

Thus from above discussion , it is clear that every case has its oven merit and demerits but one thing which is basically true is that both cases are good for small value of the parameter i.e. the degree of the polynomial , size of the field and the multiplicative order’ .The case I gives us the factorization of $x^n - 1$ into its irreducible factors but in case II we factorize a general polynomial of degree ‘n’ whereas its factors may not be irreducible.

References

[1]. Berlekamp, E.R. (1968) Algebraic Coding Theory Mc Graw-Hill.

[2]. Herstein, I N (1976), Topics in Algebra, Vikas Publishing House, New Delhi.

[3]. Khanna, Vijay K and Bhambri, S K. (1993), A Course in Abstract Algebra, Vikas Publishing House New Delhi.

[4]. Singh K. (IJMSI) Construction of some Finite Fields of order p^n over GF(p) Volume 1 Issue 1 (August. 2013) PP 44-47.

[5]. Singh K. (IOSR-JM) Factorization of some Polynomials over GF(q) / < p(x) > Vol. 17 Issue 2 (March-April 2021) PP 67-69.

[6]. Vermani L.R. (1964), Elements of Algebraic Coding Theory, CHAPMAN & HALL, MATHEMATICS.

[7]. Zameerudin Quazi and Surjeet Singh (1975), Modern Algebra, Vikas Publishing House New Delhi.