International Journal of Mathematics and Statistics Invention (IJMSI)
E-ISSN: 2321 – 4767 P-ISSN: 2321 - 4759
www.ijmsi.org Volume 7 Issue 6 || Nov. – Dec., 2019 || PP 01-06

Irreducible factors of $x^{p_1^{\alpha_1} p_2^{\alpha_2}} - 1$ over F_l

Kulvir Singh

Department of Mathematics, MNS Government College,
Bhiwani (India) Email: kulvirsheoran@yahoo.com

Abstract
Let p_1,p_2 and l be distinct odd primes and let l be a primitive root modulo $p_i^{\alpha_i}$ with $gcd(\phi(p_i^{\alpha_i}), \phi(p_j^{\alpha_j})) = 2; 1 \leq i < j \leq 2$ and gcd(l,p_i − 1) = 1. In this paper it is shown that the explicit expression of $\theta_1(x)$ from the ring $\frac{F_l[x]}{x^m-1}$ is sufficient to obtain all Gaussain periods over l-cyclotomic cosets modulo m for m = p_1p_2. In Theorems 2.5, it is shown that for computation of all irreducible factors of $x^m - 1$, $m = p_1^{\alpha_1} p_2^{\alpha_2}$ over F_l; α_1, α_2 are positive integers, it is sufficient to compute all irreducible factors of $x^{p_1p_2} - 1$ Therefore, in this paper we obtain the irreducible factors of $x^{p_1p_2} - 1$ over F_l with the help of the Gaussian periods.

Keywords: *Cyclotomic cosets; Minimal polynomials; Gaussian periods; Primitive idempotents; λ-mapping.*
Mathematics Subject Classification *(2010). 11A07; 12E20; 11T55.*

I. Introduction

The factorization of $x^m - 1$ over a finite field F_l is a problem of much interest. In coding theory, the irreducible factors of $x^m - 1$ over F_l are used in error correcting codes, secure communication, deterministic simultation of random processes and digital tracking system (see [4]). Since each irreducible factor can be used to generate a minimal cyclic code (see [1], [9]), therefore many authors have obtained the irreducible factors of $x^m - 1$ over F_l under different conditions to compute the minimum distance and the weight distribution of cyclic codes of length m. When $p|(l-1)$, Chen et al. [2] showed that the irreducible factors of $x^{2tpn} - 1$ over F_l are either binomials or trinomials. For a positive integer m, Martinez et al. [8] investigated that $x^m - 1$ can be written as a product of irreducible polynomials of the form $x^t - a$ or $x^{2t} - ax^t + b$ over F_l. Li and Cao [7] showed that the factors of $x^{2apbrc} - 1$ over F_l, where p and r are odd prime divisors of $(l-1)$, are either binomials or trinomials. In [11] Wu et al. factorized $x^m - 1$ over F_l, where $rad(d)$ does not divide $(l-1)$ and $rad(d)|(l^w - 1)$;w prime. They also counted the number of irreducible factors.

If $\eta_s(x) = \prod_{s \in C_s^{m(l)}} (x - \xi^s)$ is the minimal polynomial corresponding to the cyclotomic cosets $C_s^{m(l)}$ where ξ is a primitive mth root of unity and $O(C_s^{m(l)}) = n$. Then $\eta_s(x) = x^n - \beta_1 x^{n-1} + ... + (-1)^n \beta_n$ where β_i are sum of the products of ξ^j taken i at a time. Therefore, to compute β_i we need the sum of the form $\sum_{i \in C_s^{m(l)}} \xi^i$, where s runs over each cyclotomic cosets. As Gaussian period corresponding to $C_s^{m(l)}$ is denoted by $\sigma_s(\xi)$, where $\sigma_s(\xi) = \sum_{i \in C_s^{m(l)}} \xi^i$, therefore the different $\sigma_s(\xi)$ are used to evaluate the coefficients of $\eta_s(x)$.

Throughout the paper F_l is a finite field of order l and p_1,p_2 are distinct primes where l as a primitive root modulo $p_i^{\alpha_i}$, $gcd(\phi(p_i^{\alpha_i}), \phi(p_j^{\alpha_j}))$ = 2 and gcd(l,p_i − 1) = 1. In this paper, all the irreducible factors of $x^{p_1^{\alpha}} - 1$, $x^{p_1^{\alpha_1} p_2^{\alpha_2}} - 1$ are obtained by using the irreducible factors of $x^{p_1} - 1$, $x^{p_1p_2} - 1$. Further in Lemma 2.7 it is shown that to obtain all the irreducible factors of $x^{p_1p_2} - 1$ and $x^{p_1p_2p_3} - 1$ over F_l, the explicit expression of primitive idempotent $\theta_1^{p_1p_2}(x)$ (from $\frac{F_l[x]}{<x^{p_1p_2}-1>}$) is useful.

This paper is organized as follows. In Section 2, some definitions are given and the irreducible factors of $x^{p_1^{\alpha_1}} - 1$ over F_l are obtained. If $f(x) = \prod_{m(l)}(x - \xi^s)$, where $C_s^{m(l)}$ is a l-cyclotomic coset modulo m and ξ is a $s \in C_s$ primitive mth root of unity, then the coefficient of x^i in $f(x)$ is of the form $^{p}t_{k,i}\sigma_i(\xi)$ (see [10]), where $t_{k,i}$ are solutions of $x_1 + x_2 + ... + x_k = i$ in $C_s^{m(l)}$, i runs over each l-cyclotomic coset modulo m and $\sigma_i(\xi) = \sum_{s \in C_i^{m(l)}} \xi^s$.

Algorithm 2.10 is given to compute the irreducible factors of $x^{p_1^{\alpha_1} p_2^{\alpha_2}} - 1$ over F_l.

II. Factorization of $x^{p_1^{\alpha_1} p_2^{\alpha_2}} - 1$ over F_l

In this section we obtain all irreducible factors of $x^{p_1^{\alpha_1} p_2^{\alpha_2}} - 1$ over F_l. First we give some definitions and results which are used throughout the paper.

Denote the l-cyclotomic coset modulo m containing s; $0 \le s \le m - 1$ by $C_s^{m(l)} = \{s, sl, sl^2, ..., sl^{t-1}\}$, where t is the smallest positive integer such that $sl^t \cong s \pmod m$. The $O(C_s^{m(l)})$ denote the order of $C_s^{m(l)}$. Corresponding to each $C_s^{m(l)}$ there exist an irreducible factor of $x^m - 1$ defined as $\eta_s^m(x) = \prod_{s \in C_s^{m(l)}} (x - \xi^s)$, where ξ is a primitive mth root of unity. It is also shown that the factorisation of $x^{p_1^{\alpha_1}} - 1$ over F_l is trivial.

Definition 2.1 λ**−mapping** (Definition 2.2 [5]). Let $A_1 = \{0,1,2,...,p_1 - 1\}$, $A_2 = \{0,1,2,...,p_2 - 1\}$ and $A = \{0,1,2,...,p_1p_2\}$. Then the mapping $A_1 \times A_2 \to A$ defined by $\lambda(a_1,a_2) = a_1p_2 + a_2p_1 (mod\ p_1p_2)$ is called a λ − mapping.

Definition 2.2 (Primitive idempotent [1]) Let $R_m = \frac{F_l[x]}{x^m - 1}$ be a semisimple ring. The primitive idempotent corresponding to $C_1^{m(l)}$ denoted by $\theta_1^m(x)$ is given by $\theta_1^m(x) = \sum_{i=0}^{m-1} \epsilon_i x^i$, where $\epsilon_i = \sum_{s \in C_1^{m(l)}} \xi^{-si}$.

As l is a primitive root modulo $p_1^{\alpha_1}$, therefore, there are two l-cyclotomic cosets $C_0^{p_1(l)}$ and $C_1^{p_1(l)}$ modulo p_1. If $x^{p1} - 1 = \eta_0(x)\eta_1(x)$, where $\eta_1(x)$ is the minimal polynomial of primitive p_1th root of unity, then $x^{p_1^{\alpha_1}} - 1 = \eta_0(x) \prod_{i=0}^{n-1} \eta_1(x^{p_1^{\alpha_1 - i - 1}})$.

Theorem 2.3 The

Proof. Since l is a primitive root modulo $p_1^{\alpha_1}$, there are $n + 1$ cyclotomic cosets modulo $p_1^{\alpha_1}$, namely, $C_0^{p_1^{\alpha_1}(l)}$ and $C_{p_1^i}^{p_1^{\alpha_1}(l)}; 0 \le i \le \alpha_1 - 1$. Let β be a primitive $p_1^{\alpha_1}$th root of unity. Then $x^{p_1^{\alpha_1}} - 1 = \eta_0^*(x) \prod_{i=0}^{\alpha_1 - 1} \eta_{p_1^i}^*(x)$, where $\eta_{p_1^i}^*(x)$ is the minimal polynomial of $\beta^{p_1^i}$. Let $\delta = \beta^{p_1^i}$. Then $\delta^{p_1^{\alpha_1 - i - 1}}$ is a primitive p_1th root of unity. If $\eta_1(x)$ is the minimal polynomial of $\delta^{p_1^{\alpha_1 - i - 1}}$, then $\eta_1(x^{p_1^{\alpha_1 - i - 1}})$ is the minimal polynomial of δ. Consequently, $\eta_{p_1^i}^*(x) = \eta_1(x^{p_1^{\alpha_1 - i - 1}})$. Hence $x^{p_1^{\alpha_1}} - 1 = \eta_0(x) \prod_{i=0}^{\alpha_1 - 1} \eta_1(x^{p_1^{\alpha_1 - i - 1}})$. ◇

Note 2.4 It is easy to see that when l is a primitive root modulo $p_1^{\alpha_1}$, then $\eta_0(x) = x - 1$ and $\eta_1(x) = 1 + x + x^2 + ... + x^{p1-1}$. ◇

We now compute the irreducible factors of $x^{p1p2} - 1$ over F_l under the following conditions: For $1 \le i \le 2$, (i) l is a primitive root modulo $p^{\alpha_i\ i}$ (ii) $gcd(\phi(p_1^{\alpha_1}), \phi(p_2^{\alpha_2})) = 2$ (iii) $gcd(l, p_i - 1) = 1$. Then, by Lemma 2 [6], the order of l modulo p_1p_2 i.e. $O_{p_1p_2}(l) = \frac{\phi(p_1p_2)}{2}$. Therefore, there are five $l$cyclotomic cosets $C_0^{p_1p_2(l)}$, $C_1^{p_1p_2(l)}$, $C_a^{p_1p_2(l)}$, $C_{p_1}^{p_1p_2(l)}$ and $C_{p_2}^{p_1p_2(l)}$ modulo p_1p_2, where a is not congruent to l^t mod p_1p_2. Therefore, if $x^{p1p2} - 1 = \eta_0(x)\eta_1(x)\ \eta_a(x)\eta_{p1}(x)\eta_{p2}(x)$, where $\eta_1(x)\eta_a(x)$ is a product of minimal polynomials of β

and β^a, $\eta_{p1}(x) = 1 + x + x^2 + ... + x^{p2-1}$ is minimal polynomial of β^{p1}, $\eta_{p2}(x) = 1+x+x^2+...+x^{p1-1}$ is minimal polynomial of β^{p2}; β is a primitive p_1p_2th root of unity, then

Theorem 2.5 The $x^{p_1^{\alpha_1}p_2^{\alpha_2}} - 1 = \eta_0(x)\prod_{(i,j)=(0,0)}^{(\alpha_1-1,\alpha_2-1)}\eta_1(x^{p_1^{\alpha_1-i-1}p_2^{\alpha_2-j-1}})$ $\eta_a(x^{p_1^{\alpha_1-i-1}p_2^{\alpha_2-j-1}})\prod_{i=0}^{(\alpha_1-1)}\eta_{p_2}(x^{p_1^{\alpha_1-i-1}})\prod_{j=0}^{(\alpha_2-1)}\eta_{p_1}(x^{p_2^{\alpha_2-j-1}})$.

Proof. The $2^{\alpha_1\alpha_2+\alpha_1+\alpha_2+1}$ l-cyclotomic cosets modulo $p_1^{\alpha_1}p_2^{\alpha_2}$, are(See Theorem 1[6]), $C_0^{p_1p_2(l)}$, $C_{p_1^ip_2^j}^{p_1p_2(l)}$, $C_{ap_1^ip_2^j}^{p_1p_2(l)}$, $C_{p_1^ip_2^{\alpha_2}}^{p_1p_2(l)}$ and $C_{p_1^{\alpha_1}p_2^j}^{p_1p_2(l)}$;$0 \le i \le \alpha_1-1, 0 \le j \le \alpha_2-1$. Then $x^{p_1^{\alpha_1}p_2^{\alpha_2}}-1 = \eta_0(x)\prod_{(i,j)=(0,0)}^{(\alpha_1-1,\alpha_2-1)}\eta^*_{p_1^ip_2^j}(x)\eta^*_{ap_1^ip_2^j}(x)$ $\prod_{i=0}^{(\alpha_1-1)}\eta^*_{p_1^ip_2^{\alpha_2}}(x)\ \prod_{j=0}^{(\alpha_2-1)}\eta^*_{p_1^{\alpha_1}p_2^j}(x)$; $\eta^*_s(x)$ is the minimal polynomial corresponding to $C_s^{p_1^{\alpha_1}p_2^{\alpha_2}(l)}$.

Let γ be a primitive $p_1^{\alpha_1}p_2^{\alpha_2}$th root of unity. Then, $\eta^*_{p^ip^j}(x)\eta^*_{ap^ip^j}(x)$ is a product of minimal polynomials of $\gamma^{p_1^ip_2^j}$ and $\gamma^{api_1pj_2}$. Choose $\delta = \gamma^{p_1^ip_2^j}$ and $\delta^a = \gamma^{ap_1^ip_2^j}$. Then and $\delta^{ap_1p_2}$ are primitive p_1p_2th root of unity. Therefore, the product of their minimal polynomials is $\eta_1(x)\eta_a(x)$.

Consequently, $\eta_1(x^{p_1^{\alpha_1-i-1}p_2^{\alpha_2-j-1}})\ \eta_a(x^{p_1^{\alpha_1-i-1}p_2^{\alpha_2-j-1}})$ is a product of minimal polynomials of δ and δ^a. Hence $\eta^*_{p_1^ip_2^j}(x)\eta^*_{ap_1^ip_2^j}(x) = \eta_1(x^{p_1^{\alpha_1-i-1}p_2^{\alpha_2-j-1}})$ $\eta_a(x^{p_1^{\alpha_1-i-1}p_2^{\alpha_2-j-1}})$. The minimal polynomial of $\gamma^{p_1^ip_2^{\alpha_2}}$ is $\eta^*_{p_1^ip_2^{\alpha_2}}(x)$. If we take $\delta^* = \gamma^{p_1^ip_2^{\alpha_2}}$, then $(\delta^*)^{p_1^{\alpha_1-i-1}}$ becomes primitive p_1th root of unity, therefore, $\eta_{p_2}(x) = (1 + x + ... + x^{p_1-1})$ is its minimal polynomial. Equivalently, $\eta^*_{p_1^ip_2^{\alpha_2}}(x) = \eta_{p_2}(x^{p_1^{\alpha_1-i-1}})$.

$\eta_{p2}(x^{p_1})$ is the minimal polynomial of δ^*. Hence

Similarly, $\eta^*_{p_1^{\alpha_1}p_2^j}(x) = \eta_{p_1}(x^{p_2^{\alpha_2-j-1}})$ ◇

Lemma 2.6 Let $B = \{s_1+s_2+...+s_k | s_j$ are distinct elements of $C_s^{p1p2(l)}\}$ has $t_{k,i}$ solutions of $x_1 + x_2 + ... + x_k = i; i = 0$ or 1 or a or p_1 or $p_2; 1 \le k \le O(C_s^{p_1p_2(l)}) - 1$. Then $C_i^{p1p2(l)}$ appears $t_{k,i}$ times in B. Moreover, if

$Ps \in Csp1p2(l)$ $s = 0$, then, in B, $tk,i = tO(Csp1p2(l))-k,-i$.

Proof. Let $x_1 = s_1, x_2 = s_2, ..., x_k = s_k$ be a solution of $x_1+x_2+...+x_k = i$, then

$$s_1 + s_2 + ... + s_k = i$$

Equivalently,

$$s1lv + s2lv + ... + sklv = ilv; 0 \le v \le O(Csp1p2(l)) - 1 \quad (1)$$

In (1), the left hand side is a sum of elements of $C_s^{p_1p_2(l)}$ taking k at a time while right hand side is $C_i^{p1p2(l)}$, therefore, for each solution of $x_1+x_2+...+x_k = i$, the $C_i^{p1p2(l)}$ appears $t_{k,i}$ times in B. If,

$$s_1 + s_2 + ... + s_k + s_{k+1} + ... + s_{O(C_s^{p_1p_2(l)})} = 0; s_i \in C_s^{p_1p_2(l)}$$

and, if $s_1+s_2+...+s_k = i$, then, from above equation, $s_{k+1}+...+s_{O(C}sp_1p_2(_{l)}) =$

$-i$. Equivalently, $tk,i = tO(Csp1p2(l))-k,-i$. ⋄

Lemma 2.7 Let $\sigma_i(\xi) = {}^{P}{}_{s\in C}ip_1p_2(_l)\ \xi^s$ and, let p_1 be of $4k + 1$ type and p_2 be of $4k +3$ type. Then $\sigma_1(\xi) = \frac{1-\sqrt{-p_1p_2}}{2}$, $\sigma_a(\xi) = \frac{1+\sqrt{-p_1p_2}}{2}$, $\sigma_{p_1}(\xi) = -$1, $\sigma_{p2}(\xi) = -1$ and $\sigma_0(\xi) = 1$. Further, if p_1 and p_2 both are of $4k+3$ type, then $\sigma_1(\xi) = \frac{1+\sqrt{p_1p_2}}{2}$, $\sigma_a(\xi) = \frac{1-\sqrt{p_1p_2}}{2}$, $\sigma_{p_1}(\xi) = -1$, $\sigma_{p_2}(\xi) = -$1 and $\sigma_0(\xi) = 1$. **Proof.** By Definition 2.2, in θ_1, $\epsilon_i = \sum_{s\in C_1^{p_1p_2(l)}} \xi^{-si} = \sum_{s\in -C_1^{p_1p_2(l)}} \xi^{si} = \frac{O(C_1^{p_1p_2(l)})}{O(C_i^{p_1p_2(l)})}\sigma_{-i}(\xi$). Therefore,

$$\sigma_{-i}(\xi) = (\epsilon_i)\frac{O(C_i^{p_1p_2(l)})}{O(C_1^{p_1p_2(l)})} \qquad (2)$$

We now discuss two cases:

(i) When p_1 is $4k+1$ type and p_2 is $4k+3$ type. Then $-C_1^{p_1p_2(l)} = C_a^{p_1p_2(l)}$, $\epsilon_1 = \frac{1+\sqrt{-p_1p_2}}{2}$, $\epsilon_a = \frac{1-\sqrt{-p_1p_2}}{2}$, $\epsilon_{p_1} = -\frac{\phi(p_1)}{2}$, $\epsilon_{p_2} = -\frac{\phi(p_2)}{2}$ and $\epsilon_0 = \frac{\phi(p_1p_2)}{2}$ (for the values of ϵ_i see Theorem 3[1]). Therefore, by (2) $\sigma_1(\xi) = \frac{1-\sqrt{-p_1p_2}}{2}$, $\sigma_a(\xi) = \frac{1+\sqrt{-p_1p_2}}{2}$, $\sigma_{p_1}(\xi) = -1$, $\sigma_{p_2}(\xi) = -$1 and $\sigma_0(\xi) = 1$.

(ii) p_1 and p_2 both are of $4k + 3$ type. Then, $-C_1^{p_1p_2(l)} = C_1^{p_1p_2(l)}$, $\epsilon_1 = \frac{1+\sqrt{p_1p_2}}{2}$, $\epsilon_a = \frac{1-\sqrt{p_1p_2}}{2}$, $\epsilon_{p_1} = -\frac{\phi(p_1)}{2}$, $\epsilon_{p_2} = -\frac{\phi(p_2)}{2}$ and $\epsilon_0 = \frac{\phi(p_1p_2)}{2}$. Again by (2) $\sigma_1(\xi) = \frac{1+\sqrt{p_1p_2}}{2}$, $\sigma_a(\xi) = \frac{1-\sqrt{p_1p_2}}{2}$, $\sigma_{p_1}(\xi) = -1$, $\sigma_{p_2}(\xi) = -$1 and $\sigma_0(\xi) = 1$.⋄

Theorem 2.8 The $\eta_s(x) = \sum_{k=0}^{O(C_s^{p_1p_2(l)})}(-1)^k a_k x^{O(C_s^{p_1p_2(l)})-k}$, where

$$a_k = \begin{cases} t_{k,0} + t_{k,1}\frac{1-\sqrt{-p_1p_2}}{2} + t_{k,a}\frac{1+\sqrt{-p_1p_2}}{2} - t_{k,p_1} - t_{k,p_2} & ;p_1 = 4k+1 \text{ and } p_2 = 4k+3 \\ t_{k,0} + t_{k,1}\frac{1+\sqrt{p_1p_2}}{2} + t_{k,a}\frac{1-\sqrt{p_1p_2}}{2} - t_{k,p_1} - t_{k,p_2} & ;p_1 = 4k+3 \text{ and } p_2 = 4k+3 \end{cases}.$$

Proof. The $\eta_s(x) = {}^{Q}{}_{s\in C}sp_1p_2(_l)(x - \xi^s)$, where ξ is a primitive p_1p_2th root of unity. Since the order of $C_s^{p1p2(l)}$ is $O(C_s^{p1p2(l)})$, the degree of $\eta_s(x)$ is $O(C_s^{p_1p_2(l)})$. Let $\eta_s(x) = \sum_{k=0}^{O(C_s^{p_1p_2(\ )})}(-1)^k a_k x^{O(C_s^{p_1p_2(\ )})-k}$, where a_k is a sum of products of its roots taking k at a time. Therefore, a_k is a sum of terms of form $\xi s1+s2+...+sk;si \in Csp1p2(l)$. Then, by Lemma 2.6, $ak = tk,0\sigma0(\xi) + tk,1\sigma1(\xi) + tk,a\sigma a(\xi) + tk,p1\sigma p1(\xi) + tk,p2\sigma p2(\xi)$. By Lemma 2.7, the

$$a_k = \begin{cases} t_{k,0} + t_{k,1}\frac{1-\sqrt{-p_1p_2}}{2} + t_{k,a}\frac{1+\sqrt{-p_1p_2}}{2} - t_{k,p_1} - t_{k,p_2} & ;p_1 = 4k+1 \text{ and } p_2 = 4k+3 \\ t_{k,0} + t_{k,1}\frac{1+\sqrt{p_1p_2}}{2} + t_{k,a}\frac{1-\sqrt{p_1p_2}}{2} - t_{k,p_1} - t_{k,p_2} & ;p_1 = 4k+3 \text{ and } p_2 = 4k+3 \end{cases}.\diamond$$

Remark 2.9 (i) Trivially, $\eta_0(x) = x - 1, \eta_{p1}(x) = 1 + x + ... + x^{p2-1}$ and $\eta_{p2}(x) = 1 + x + ... + x^{p1-1}$.

(ii) If p_1 and p_2 both are of $4k + 3$ form, then $-C_1^{p_1p_2(l)} = C_1^{p_1p_2(l)}$. Therefore, by Lemma 2.6, we have to compute $t_{k,i}$ for $1 \le k \le \frac{\phi(p_1p_2)}{4}$ as

$t_{k,i} = t\phi(p_1p_2) = k,i$
4

a. Algorithm to compute the irreducible factors of $x^{p_1p_2} - 1$

We have following algorithm to compute the $\eta_s(x) = {}^{Q}{}_{s\in C} sp_1p_2(_l)(x - \xi^s)$.

Step 1. Compute $B = \{s_1+s_2+...+s_k | s_j$ are distinct elements of $C_s^{p_1p_2(l)}\}$ Step 2. Compute $t_{k,i}$, where $t_{k,i}$ are number of solutions of $x_1 + x_2 + ... + x_k = i; i = 0$ or 1 or a or p_1 or p_2

in B.

Step 3. Compute a_k as discussed in Theorem 2.8.

l

$$\eta_s(x) = \sum_{k=0}^{O(C_s^{p_1p_2(\ )})} (-1)^k a_k x^{O(C_s^{p_1p_2(l)})-k}$$

Step 4. The.

Step 5. Stop.

III. Example

Example In this example we find all the irreducible factors of $x^{35} - 1$ over F_{17}. The 5 distinct 17-cyclotomic cosets modulo 35 are $C_0^{35}, C_1^{35}, C_2^{35}, C_5^{35}$ and C_7^{35} . As 17 is a primitive root modulo both $5^{\alpha 1}$ and $7^{\alpha 2}$, therefore, we compute the irreducible factors of $x^{35} - 1$ over F_{17}. Let γ be a primitive 35th root of unity. As order of 17 modulo 35 is 12, we need to compute $a_k; 1 \le k \le 11$. By Lemma 2.7, $\sigma_0(\gamma) = 1, \sigma_1(\gamma) = 7, \sigma_2(\gamma) = 11, \sigma_5(\gamma) = -1$ and $\sigma_7(\gamma) = -1$ Therfore, by Lemma 2.6, $t1,0 = 0, t1,1 = 1, t1,2 = 0, t1,5 = 0, t1,7 = 0$, and $a1 = \sigma1(\gamma) = 7$, $t2,0 = 0, t2,1 = 2, t2,2 = 1, t2,5 = 3, t2,7 = 3$, and $a2 = t2,0\sigma0(\gamma)+t2,1\sigma1(\gamma)+$

$t2,2\sigma2(\gamma) + t2,5\sigma5(\gamma) + t2,7\sigma7(\gamma) = 2$, $t3,0 = 0, t3,1 = 6, t3,2 = 7, t3,5 = 6, t3,7 = 7$, and $a3 = t3,0\sigma0(\gamma)+t3,1\sigma1(\gamma)+$

$t3,2\sigma2(\gamma) + t3,5\sigma5(\gamma) + t3,7\sigma7(\gamma) = 4$, $t4,0 = 15, t4,1 = 12, t4,2 = 15, t4,5 = 16, t4,7 = 15$, and $a4 = t4,0\sigma0(\gamma) +$

$t4,1\sigma1(\gamma) + t4,2\sigma2(\gamma) + t4,5\sigma5(\gamma) + t4,7\sigma7(\gamma) = 12$, $t5,0 = 24, t5,1 = 22, t5,2 = 25, t5,5 = 20, t5,7 = 21$, and $a5 = t5,0\sigma0(\gamma) +$

$t5,1\sigma1(\gamma) + t5,2\sigma2(\gamma) + t5,5\sigma5(\gamma) + t5,7\sigma7(\gamma) = 4$, $t6,0 = 38, t6,1 = 26, t6,2 = 26, t6,5 = 27, t6,7 = 25$, and $a6 = t6,0\sigma0(\gamma) +$

$t6,1\sigma1(\gamma) + t6,2\sigma2(\gamma) + t6,5\sigma5(\gamma) + t6,7\sigma7(\gamma) = 12$, $t7,0 = 24, t7,1 = 25, t7,2 = 22, t7,5 = 20, t7,7 = 21$, and $a7 = t7,0\sigma0(\gamma) +$

$t7,1\sigma1(\gamma) + t7,2\sigma2(\gamma) + t7,5\sigma5(\gamma) + t7,7\sigma7(\gamma) = 9$, $t8,0 = 15, t8,1 = 15, t8,2 = 12, t8,5 = 16, t8,7 = 15$, and $a8 = t8,0\sigma0(\gamma) +$

$t8,1\sigma1(\gamma) + t8,2\sigma2(\gamma) + t8,5\sigma5(\gamma) + t8,7\sigma7(\gamma) = 0$, $t9,0 = 0, t9,1 = 7, t9,2 = 6, t9,5 = 6, t9,7 = 7$, and $a9 = t9,0\sigma0(\gamma)+t9,1\sigma1(\gamma)+$

$t9,2\sigma2(\gamma) + t9,5\sigma5(\gamma) + t9,7\sigma7(\gamma) = 0$, $t10,0 = 0, t10,1 = 1, t10,2 = 2, t10,5 = 3, t10,7 = 3$, and $a10 = t10,0\sigma0(\gamma) +$

$t10,1\sigma1(\gamma) + t10,2\sigma2(\gamma) + t10,5\sigma5(\gamma) + t10,7\sigma7(\gamma) = 6$, $t11,0 = 0, t11,1 = 0, t11,2 = 1, t11,5 = 0, t11,7 = 0$, and $a11 = t11,0\sigma0(\gamma) +$

$t11,1\sigma1(\gamma) + t11,2\sigma2(\gamma) + t11,5\sigma5(\gamma) + t11,7\sigma7(\gamma) = 11$,

Hence

$$\eta_1^{35}(x) = x^{12} - 7x^{11} + 2x^{10} - 4x^9 + 12x^8 - 4x^7 + 12x^6 - 9x^5 + 6x^2 - 11x_{+1},$$

Since the roots of η_2^{35} are reciprocal of roots of η_1^{35}, therefore,

$$\eta_2^{35}(x) = x^{12} - 11x^{11} + 6x^{10} - 9x^7 + 12x^6 - 4x^5 + 12x^4 - 4x^3 + 2x^2 - 7x + 1.$$

Further, by Remark 2.9(i), it is easy to see that

$$\eta_5^{35}(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x_{+\,1},$$

$$\eta_7^{35}(x) = x^4 + x^3 + x^2 + x_{+\,1}, \text{ and}$$

$\eta_0^{35}(x) = x -$1. Hence $x^{35} - 1 = (x-1)(x^{12} - 7x^{11} + 2x^{10} - 4x^9 + 12x^8 - 4x^7 + 12x^6 - 9x^5 + 6x^2 - 11x + 1)(x^{12} - 11x^{11} + 6x^{10} - 9x^7 + 12x^6 - 4x^5 + 12x^4 - 4x^3 + 2x^2 - 7x + 1)(x^4 + x^3 + x^2 + x + 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$.

By Theorem 2.5, $x^{5^{\alpha_1}7^{\alpha_2}} - 1 = (x-1)\prod_{(i,j)=(0,0)}^{(\alpha_1-1,\alpha_2-1)} (x^{12(5^{\alpha_1-i-1}7^{\alpha_2-j-1})} -$

$7x11(5\alpha 1-i-17\alpha 2-j-1)+2x10(5\alpha 1-i-17\alpha 2-j-1)-4x9(5\alpha 1-i-17\alpha 2-j-1)+12x8(5\alpha 1-i-17\alpha 2-j-1)-$
$4x7(5\alpha 1-i-17\alpha 2-j-1)+12x6(5\alpha 1-i-17\alpha 2-j-1)-9x5(5\alpha 1-i-17\alpha 2-j-1)+6x2(5\alpha 1-i-17\alpha 2-j-1)-$
$11x(5\alpha 1-i-17\alpha 2-j-1)+1)(x12(5\alpha 1-i-17\alpha 2-j-1)-11x11(5\alpha 1-i-17\alpha 2-j-1)+6x10(5\alpha 1-i-17\alpha 2-j-1)-$
$9x7(5\alpha 1-i-17\alpha 2-j-1)+12x6(5\alpha 1-i-17\alpha 2-j-1)-4x5(5\alpha 1-i-17\alpha 2-j-1)+12x4(5\alpha 1-i-17\alpha 2-j-1)-$
$4x3(5\alpha 1-i-17\alpha 2-j-1)+2x2(5\alpha 1-i-17\alpha 2-j-1)-7x(5\alpha 1-i-17\alpha 2-j-1)+1)_{Q}{}^{\alpha}{}_{j=0}2-{}^{1}(x4(7\alpha 2-j-1)+$
$x3(7\alpha 2-j-1)+x2(7\alpha 2-j-1)+x7\alpha 2-j-1+1)_{Q}\alpha_{i=0}1-1(x6(5\alpha 1-i-1)+x5(5\alpha 1-i-1)+x4(5\alpha 1-i-1)+ x3(5\alpha^{1}-i-1^{)}+$
$x2(5\alpha^{1}-i-1^{)}+ x5\alpha^{1}-i-1 + 1).$

References

[1]. G.K. Bakshi and M. Raka, Minimal cyclic codes of length p^nq, *Finite Fields Appl.* **9** (2003) 432-448.

[2]. B. Chen, L. Li and R. Tuerhong, Explicit factorization of $x^{2mpn}-1$ over a finite field, *Finite Fields Appl.* **24** (2013) 95-104.

[3]. P. Devi and P. Kumar, Cyclotomic cosets and primitive idempotents in semisimple ring, *Commun. Algeb*. Doi 10.1080/00927872.2019.1570234.

[4]. S.W. Golomb, *Shift register sequences*, (Holden-Day, Inc. San Francisco 1967).

[5]. P. Kumar and S.K. Arora, λ-mapping and primitive idempotents in semisimple ring $\mathfrak{R}_m$, *Commun. Algeb*. **41** (2013) 3679-3694.

[6]. P. Kumar, S.K. Arora and S. Batra, Primitive idempotents and generator polynomials of some minimal cyclic codes of length p^nq^m, *Int. J. Inform. Coding Theo.* **2** (2014) 191-217.

[7]. F. Li and X. Cao, Explicit Factorization of $x^{2apbrc}-1$ over a finite field, *Int. J. Pure and Appl. Math.* **97** (2014) 67-77.

[8]. F. Martinez, C. Vergara and L. Oliveira, Explicit Factorization of $x^n-1 \in F_q[x]$, *Des. Codes Cryptogr*. **77** (2015) 277-286.

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

[10]. T. Strorer, *Cyclotomy and Difference Sets*, (Markhan Publishing Company, Chicago 1967).

[11]. Y. Wu, Q. Yue and S. Fan, Further factorization of x^n-1 over a finite field, *Finite Fields Appl.* **54** (2018) 197-215.