International Journal of Mathematics and Statistics Invention (IJMSI)
e-ISSN: 2321- 4767 P-ISSN: 2321-4759
www.ijmsi.org Volume 8 Issue 2 || Feb, 2020 || PP-22-34

Irreducible factors of $x^{p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}} - 1$ over F_l

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

Abstract

Let p_1, p_2, p_3 and l be distinct odd primes and let l be a primitive root modulo $p_i^{\alpha_i}$ with $gcd\left(\phi\left(p_i^{\alpha_i}\right), \phi\left(p_j^{\alpha_j}\right)\right) = 2; 1 \le i < j \le 3$ and $gcd\left(l, p_i - 1\right) = 1$. 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 $m = p_1 p_2 p_3$. In Theorems 2.5, it is shown that for computation of all irreducible factors of $x^m - 1$, $m = p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3}$ over F_l ; α_1 , α_2 and α_3 are positive integers, it is sufficient to compute all irreducible factors of $x^{p_1 p_2 p_3} - 1$ over F_l. Therefore, in this paper we obtain the irreducible factors of $x^{p_1 p_2 p_3} - 1$ 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 simulation 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 $x^{2^t p^n} - 1$ 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 $x^{2^a p^b r^c} - 1$ 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 $\eta_s(x) = \prod_{s \in C_s^{m(l)}} \left(x - \xi^s\right)$ is the minimal polynomial corresponding to the cyclotomic cosets $C_s^{m(l)}$ where ξ is a primitive mth root of unity and $O\left(C_s^{m(l)}\right) = n$. Then $\eta_s(x) = x^n - \beta_1 x^{n-1} + \ldots + (-1)^n \beta_n$ 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 $\eta_s(x)$.

Hereafter, let F_l be a finite field of order l and p_1, p_2, p_3 be distinct primes where l as a primitive root modulo $p_i^{\alpha_i}$, $gcd\left(\left(p_i^{\alpha_i}\right),\left(p_j^{\alpha_j}\right)\right)=2$ and $gcd(l, p_i-1)=1$. In this paper, all the irreducible $x^{p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}}-1$ are computed with the help of irreducible factors of $x^{p_1p_2p_3}-1$. Further in Theorem 2.9, it is shown that to obtain all the irreducible factors of $x^{p_1p_2p_3}-1$ over F_l, the explicit expression of primitive idempotent $\theta_1^{p_1p_2p_3}(x)$ (from $\frac{F_l[x)}{\langle x^{p_1p_2p_3}-1\rangle}$) is useful.

This paper is organized as follows. In Section 2, we factorize $x^{p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}}-1$ over F_l. In the last section all the results are discussed by an example.

2 Factorization of $x^{p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}}-1$ 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 $s; 0\le s\le m\le 1$ by $C_s^{m(l)}=\{s, sl, sl^2, \ldots, sl^{t-1}\}$, where t is the smallest positive integer such that $sl^t\cong s(\mathrm{mod}m)$. The $O\left(C_s^{m(l)}\right)$ 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 $\eta_s^m(x)=\prod_{s\in C_s^{m(l)}}\left(x-\xi^s\right)$, where ξ is a primitive m-th root of unity. It is also shown that the factorization of $x^{p_1^{\alpha_1}}-1$ over F_l is trivial.

Definition 2.1 $\lambda-$mapping (Definition 2.2 [5]). Let $A_1=\{0,1,2,\ldots,p_1-1\}$, $A_2=\{0,1,2,\ldots,p_2-1\}$, $A_3=\{0,1,2,\ldots,p_3-1\}$ and $A=\{0,1,2,\ldots,p_1p_2p_3-1\}$. Then the mapping $A_1\times A_2\times A_3\to A$ defined by $\lambda(a_1,a_2,a_3)=a_1p_2p_3+a_2p_1p_3+a_3p_1p_2(mod p_1p_2p_3)$ is called a $\lambda-$mapping.

Definition 2.2 (Primitive idempotent [1]) Let $R_m=\frac{F_l[x)}{x^m-1}$ be a semi-simple 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 $x^{p_1}-1=\eta_0(x)\eta_1(x)$, where $\eta_1(x)$ is the minimal polynomial of primitive p_1 th root of unity, then

Theorem 2.3 The $x^{p_1^{\alpha_1}}-1=\eta_0(x)\prod_{i=0}^{n-1}\eta_1\left(x^{p_1^{\alpha_1-i}-1}\right)$.

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 $C_{p_1^i}^{p_1^{\alpha_1}}(l); 0 \le i \le \alpha_1 \quad 1$. Let β be a primitive $p_1^{\alpha_1}$ th root of unity. Then $x^{p_1^{\alpha_1}} - 1 = \eta_0(x)\prod_{i=0}^{\alpha_1} \eta_{p_1^i}(x)$, 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_1 th root of unity. If $\eta_1(x)$ is the minimal polynomial of $\delta^{p_1^{\alpha_1 - i - 1}}$, then $\eta_1\left(x^{p_1^{\alpha_1 - i - 1}}\right)$ is the minimal polynomial of δ. Consequently, $\eta_{p_1^i}(x) = \eta_1\left(x^{p_1^{\alpha_1 - i - 1}}\right)$. Hence $x^{p_1^{\alpha_1}} - 1 = \eta_0(x)\prod_{i=0}^{\alpha_1 - 1} \eta_1\left(x^{p_1^{\alpha_1 - i - 1}}\right)$. ◊

For $1 \le i, j \le 3$, let l be a primitive root modulo $p_i^{\alpha_i}$, with $gcd\left(O_{p_i^{\alpha_i}}(l), O_{p_j^{\alpha_j}}(l)\right) = 2$, $gcd(l, p_i - 1) = 1$. By Theorem 2.6[5], it is easy to see that the fourteen l -cyclotomic cosets modulo $p_1 p_2 p_3$ can be written as: $C_0^{p_1p_2p_3(l)}, C_1^{p_1p_2p_3(l)}, C_a^{p_1p_2p_3(l)}, C_b^{p_1p_2p_3(l)}, C_c^{p_1p_2p_3(l)}, C_{p_1}^{p_1p_2p_3(l)}, C_{ap_1}^{p_1p_2p_3(l)}, C_{p_2}^{p_1p_2p_3(l)}, C_{bp_2}^{p_1p_2p_3(l)}, C_{p_3}^{p_1p_2p_3(l)}, C_{cp_3}^{p_1p_2p_3(l)}$, $C_{p_1p_2}^{p_1p_2p_3(l)}, C_{p_2p_3}^{p_1p_2p_3(l)}, C_{p_1p_3}^{p_1p_2p_3(l)}$, where l^{n_1}, al^{n_2}, bl^{n_3} and cl^{n_4} are pairwise incongruent modulo $p_1 p_2 p_3$. Then, there are following observations:

Observation 2.4 (i) If $p_1 = 4k+3$ form, $p_2 = 4k+1$ form and $p_3 = 4k+3$ form then $-C_1^{p_1p_2p_3(l)} = C_a^{p_1p_2p_3(l)}$ (or $-C_1^{p_1p_2p_3(l)} = C_b^{p_1p_2p_3(l)}$ or $-C_1^{p_1p_2p_3(l)} = C_c^{p_1p_2p_3(l)}$), $-C_b^{p_1p_2p_3(l)} = C_c^{p_1p_2p_3(l)}$ (or $-C_a^{p_1p_2p_3(l)} = C_c^{p_1p_2p_3(l)}$ or $-C_a^{p_1p_2p_3(l)} = C_b^{p_1p_2p_3(l)}$), $-C_{p_1}^{p_1p_2p_3(l)} = C_{ap_1}^{p_1p_2p_3(l)}$, $-C_{p_2}^{p_1p_2p_3(l)} = C_{p_2}^{p_1p_2p_3(l)}$, $-C_{bp_2}^{p_1p_2p_3(l)} = C_{bp_2}^{p_1p_2p_3(l)}$, $-C_{p_3}^{p_1p_2p_3(l)} = C_{cp_3}^{p_1p_2p_3(l)}$, $-C_{p_1p_2}^{p_1p_2p_3(l)} = C_{p_1p_2}^{p_1p_2p_3(l)}$, $-C_{p_1p_3}^{p_1p_2p_3(l)} = C_{p_1p_3}^{p_1p_2p_3(l)}$ and $-C_{p_2p_3}^{p_1p_2p_3(l)} = C_{p_2p_3}^{p_1p_2p_3(l)}$.

(ii) If all p_i's are $4k+3$ form then $-C_1^{p_1p_2p_3(l)} = C_1^{p_1p_2p_3(l)}$, $-C_a^{p_1p_2p_3(l)} = C_a^{p_1p_2p_3(l)}$, $-C_b^{p_1p_2p_3(l)} = C_b^{p_1p_2p_3(l)}$, $-C_c^{p_1p_2p_3(l)} = C_c^{p_1p_2p_3(l)}$, $-C_{p_1}^{p_1p_2p_3(l)} = C_{p_1}^{p_1p_2p_3(l)}$, $-C_{ap_1}^{p_1p_2p_3(l)} = C_{ap_1}^{p_1p_2p_3(l)}$, $-C_{p_2}^{p_1p_2p_3(l)} = C_{p_2}^{p_1p_2p_3(l)}$, $-C_{bp_2}^{p_1p_2p_3(l)} = C_{bp_2}^{p_1p_2p_3(l)}$, $-C_{p_3}^{p_1p_2p_3(l)} = C_{p_3}^{p_1p_2p_3(l)}$, $-C_{cp_3}^{p_1p_2p_3(l)} = C_{cp_3}^{p_1p_2p_3(l)}$, $-C_{p_1p_2}^{p_1p_2p_3(l)} = C_{p_1p_2}^{p_1p_2p_3(l)}$, $-C_{p_1p_3}^{p_1p_2p_3(l)} = C_{p_1p_3}^{p_1p_2p_3(l)}$ and $-C_{p_2p_3}^{p_1p_2p_3(l)} = C_{p_2p_3}^{p_1p_2p_3(l)}$.

Let $x^{p_1p_2p_3} - 1 = \eta_0(x)\eta_1(x)\eta_a(x)\eta_b(x)\eta_c(x)\eta_{p_1}(x)\eta_{ap_1}(x)\eta_{p_2}(x)\eta_{bp_2}(x)\eta_{p_3}(x)\eta_{cp_3}(x)\eta_{p_1p_2}(x)$ $\eta_{p_1p_3}(x)\eta_{p_2p_3}(x)$, then

Theorem 2.5 The

$$x^{p_1^{\alpha_1}p_2^{\alpha_2}p_3^{\alpha_3}} - 1 = \eta_0(x)\prod_{(i,j,k)=(0,0,0)}^{(\alpha_1-1,\alpha_2-1,\alpha_3-1)} \eta_1\left(x^{p_1^{\alpha_1-i-1}p_2^{\alpha_2-j-1}p_3^{\alpha_3-k-1}}\right)$$

$$\eta_a\left(x^{p_1^{\alpha_1-i-1}p_2^{\alpha_2-j-1}p_3^{\alpha_3-k-1}}\right)\eta_b\left(x^{p_1^{\alpha_1-i-1}p_2^{\alpha_2-j-1}p_3^{\alpha_3-k-1}}\right)\eta_c\left(x^{p_1^{\alpha_1-i-1}p_2^{\alpha_2-j-1}p_3^{\alpha_3-k-1}}\right)$$

$$\prod_{(i,j)=(0,0)}^{(\alpha_1-1,\alpha_2-1)} \eta_{p_3}\left(x^{p_1^{\alpha_1-i-1}p_2^{\alpha_2-j-1}}\right)\eta_{cp_3}\left(x^{p_1^{\alpha_1-i-1}p_2^{\alpha_2-j-1}}\right)\prod_{(i,k)=(0,0)}^{(\alpha_1-1,\alpha_3-1)} \eta_{p_2}\left(x^{p_1^{\alpha_1-i-1}p_3^{\alpha_3-k-1}}\right)\eta_{bp_2}\left(x^{p_1^{\alpha_1-i-1}p_3^{\alpha_3-k-1}}\right)$$

$$\prod_{(j,k)=(0,0)}^{(\alpha_2-1,\alpha_3-1)} \eta_{p_1}\left(x^{p_2^{\alpha_2-j-1}p_3^{\alpha_3-k-1}}\right)\eta_{ap_1}\left(x^{p_2^{\alpha_2-j-1}p_3^{\alpha_3-k-1}}\right)\prod_{l=0}^{\alpha_1-1} \eta_{p_2p_3}\left(x^{p_1^{\alpha_1-i-1}}\right)\prod_{j=0}^{\alpha_2-1} \eta_{p_1p_3}\left(x^{p_2^{\alpha_2-j-1}}\right)\prod_{k=0}^{\alpha_3-1} \eta_{p_1p_2}\left(x^{p_3^{\alpha_3-k-1}}\right).$$

Lemma 2.6 Let $B = \{s_1 + s_2 + ... + s_k \vee s_j$ are distinct elements of $C_s^{p_1 p_2 p_3(l)}\}$ has $t_{k,i}$ solutions of $x_1 + x_2 + \ldots + x_k = i$; i represents each cyclotomic coset modulo $p_1 p_2 p_3$. Then $C_i^{p_1 p_2 p_3(l)}$ appears $t_{k,i}$ times in B. Moreover, if $\sum_{s \in C_i^{p_1 p_2 p_3(l)}} s = 0$, then, in B, $t_{k,i} = t_{O\left(C_s^{p_1 p_2 p_3(l)}\right)-k,-i}$.

Theorem 2.7 Let $p_1 = 4k+3$, $p_2 = 4k+1$ and $p_3 = 4k+3$. Then $\theta_1(x) = \sum \epsilon_i \sigma_i$, where the sum runs over each l-cyclotomic coset modulo $p_1 p_2 p_3$ and $\epsilon_0 = \frac{\phi(p_1 p_2 p_3)}{4}$, $\epsilon_{p_1 p_2} = -\frac{\phi(p_1 p_2)}{4}$, $\epsilon_{p_1 p_3} = -\frac{\phi(p_1 p_3)}{4}$,
$\epsilon_{p_2 p_3} = -\frac{\phi(p_2 p_3)}{4}$, $\epsilon_{p_1} = \frac{\phi(p_1)\left(1+\sqrt{-p_2 p_3}\right)}{4}$, $\epsilon_{a p_1} = \frac{\phi(p_1)\left(1-\sqrt{-p_2 p_3}\right)}{4}$, $\epsilon_{p_2} = \frac{\phi(p_2)\left(1-\sqrt{p_1 p_3}\right)}{4}$,
$\epsilon_{b p_2} = \frac{\phi(p_2)\left(1+\sqrt{p_1 p_3}\right)}{4}$, $\epsilon_{p_3} = \frac{\phi(p_3)\left(1+\sqrt{-p_1 p_2}\right)}{4}$, $\epsilon_{c p_3} = \frac{\phi(p_3)\left(1-\sqrt{-p_1 p_2}\right)}{4}$,
$\epsilon_1 = \frac{-\left(1-\sqrt{-p_1 p_2}-\sqrt{p_1 p_3}+\sqrt{-p_2 p_3}\right)}{4}$, $\epsilon_a = \frac{-\left(1-\sqrt{-p_1 p_2}+\sqrt{p_1 p_3}-\sqrt{-p_2 p_3}\right)}{4}$,
$\epsilon_b = \frac{-\left(1+\sqrt{-p_1 p_2}+\sqrt{p_1 p_3}+\sqrt{-p_2 p_3}\right)}{4}$ and $\epsilon_c = \frac{-\left(1+\sqrt{-p_1 p_2}-\sqrt{p_1 p_3}-\sqrt{-p_2 p_3}\right)}{4}$.

Proof. By Theorem 2.6[5], let the fourteen l-cyclotomic cosets modulo $p_1 p_2 p_3$ be

$$\lambda\left(C_1^{p_1}(l^2) \times C_l^{p_2}(l^2) \times C_l^{p_3}(l^2)\right) \cup \lambda\left(C_l^{p_1}(l^2) \times C_1^{p_2}(l^2) \times C_1^{p_3}(l^2)\right) = C_1^{p_1 p_2 p_3}(l),$$

$$\lambda\left(C_1^{p_1}(l^2) \times C_l^{p_2}(l^2) \times C_1^{p_3}(l^2)\right) \cup \lambda\left(C_l^{p_1}(l^2) \times C_1^{p_2}(l^2) \times C_l^{p_3}(l^2)\right) = C_a^{p_1 p_2 p_3}(l),$$

$$\lambda\left(C_1^{p_1}(l^2) \times C_1^{p_2}(l^2) \times C_1^{p_3}(l^2)\right) \cup \lambda\left(C_l^{p_1}(l^2) \times C_l^{p_2}(l^2) \times C_l^{p_3}(l^2)\right) = C_b^{p_1 p_2 p_3}(l),$$

$$\lambda\left(C_1^{p_1}(l^2) \times C_1^{p_2}(l^2) \times C_l^{p_3}(l^2)\right) \cup \lambda\left(C_l^{p_1}(l^2) \times C_l^{p_2}(l^2) \times C_1^{p_3}(l^2)\right) = C_c^{p_1 p_2 p_3}(l),$$

$$\lambda\left(C_0^{p_1}(l^2) \times C_1^{p_2}(l^2) \times C_l^{p_3}(l^2)\right) \cup \lambda\left(C_0^{p_1}(l^2) \times C_l^{p_2}(l^2) \times C_1^{p_3}(l^2)\right) = C_{ap_1}^{p_1 p_2 p_3}(l),$$

$$\lambda\left(C_0^{p_1}(l^2) \times C_l^{p_2}(l^2) \times C_l^{p_3}(l^2)\right) \cup \lambda\left(C_0^{p_1}(l^2) \times C_1^{p_2}(l^2) \times C_1^{p_3}(l^2)\right) = C_{p_1}^{p_1 p_2 p_3}(l),$$

$$\lambda\left(C_1^{p_1}\left(l^2\right)\times C_0^{p_2}\left(l^2\right)\times C_l^{p_3}\left(l^2\right)\right)\cup\lambda\left(C_l^{p_1}\left(l^2\right)\times C_0^{p_2}\left(l^2\right)\times C_1^{p_3}\left(l^2\right)\right)=C_{p_2}^{p_1p_2p_3}(l),$$

$$\lambda\left(C_1^{p_1}\left(l^2\right)\times C_0^{p_2}\left(l^2\right)\times C_1^{p_3}\left(l^2\right)\right)\cup\lambda\left(C_l^{p_1}\left(l^2\right)\times C_0^{p_2}\left(l^2\right)\times C_l^{p_3}\left(l^2\right)\right)=C_{bp_2}^{p_1p_2p_3}(l),$$

$$\lambda\left(C_1^{p_1}\left(l^2\right)\times C_1^{p_2}\left(l^2\right)\times C_0^{p_3}\left(l^2\right)\right)\cup\lambda\left(C_l^{p_1}\left(l^2\right)\times C_l^{p_2}\left(l^2\right)\times C_0^{p_3}\left(l^2\right)\right)=C_{p_3}^{p_1p_2p_3}(l),$$

$$\lambda\left(C_1^{p_1}\left(l^2\right)\times C_l^{p_2}\left(l^2\right)\times C_0^{p_3}\left(l^2\right)\right)\cup\lambda\left(C_l^{p_1}\left(l^2\right)\times C_1^{p_2}\left(l^2\right)\times C_0^{p_3}\left(l^2\right)\right)=C_{cp_3}^{p_1p_2p_3}(l),$$

$$\lambda\left(C_0^{p_1}\left(l^2\right)\times C_0^{p_2}\left(l^2\right)\times C_1^{p_3}\left(l^2\right)\right)\cup\lambda\left(C_0^{p_1}\left(l^2\right)\times C_0^{p_2}\left(l^2\right)\times C_l^{p_3}\left(l^2\right)\right)=C_{p_1p_2}^{p_1p_2p_3}(l),$$

$$\lambda\left(C_0^{p_1}\left(l^2\right)\times C_1^{p_2}\left(l^2\right)\times C_0^{p_3}\left(l^2\right)\right)\cup\lambda\left(C_0^{p_1}\left(l^2\right)\times C_l^{p_2}\left(l^2\right)\times C_0^{p_3}\left(l^2\right)\right)=C_{p_1p_3}^{p_1p_2p_3}(l)$$

and

$$\lambda\left(C_1^{p_1}\left(l^2\right)\times C_0^{p_2}\left(l^2\right)\times C_0^{p_3}\left(l^2\right)\right)\cup\lambda\left(C_l^{p_1}\left(l^2\right)\times C_0^{p_2}\left(l^2\right)\times C_0^{p_3}\left(l^2\right)\right)=C_{p_2p_3}^{p_1p_2p_3}(l).$$

By Theorem 3.4[3], $\epsilon_0=\frac{\phi(p_1p_2p_3)}{4}$, $\epsilon_{p_1p_2}=-\frac{\phi(p_1p_2)}{4}$, $\epsilon_{p_1p_3}=-\frac{\phi(p_1p_3)}{4}$, $\epsilon_{p_2p_3}=-\frac{\phi(p_2p_3)}{4}$,
$\epsilon_{p_1}=\frac{\phi(p_1)\left(1+\sqrt{-p_2p_3}\right)}{4}$, $\epsilon_{ap_1}=\frac{\phi(p_1)\left(1-\sqrt{-p_2p_3}\right)}{4}$, $\epsilon_{p_2}=\frac{\phi(p_2)\left(1-\sqrt{p_1p_3}\right)}{4}$,
$\epsilon_{bp_2}=\frac{\phi(p_2)\left(1+\sqrt{p_1p_3}\right)}{4}$, $\epsilon_{p_3}=\frac{\phi(p_3)\left(1+\sqrt{-p_1p_2}\right)}{4}$, $\epsilon_{cp_3}=\frac{\phi(p_3)\left(1-\sqrt{-p_1p_2}\right)}{4}$,
$\epsilon_1=\frac{-\left(1-\sqrt{-p_1p_2}-\sqrt{p_1p_3}+\sqrt{-p_2p_3}\right)}{4}$, $\epsilon_a=\frac{-\left(1-\sqrt{-p_1p_2}+\sqrt{p_1p_3}-\sqrt{-p_2p_3}\right)}{4}$,
$\epsilon_b=\frac{-\left(1+\sqrt{-p_1p_2}+\sqrt{p_1p_3}+\sqrt{-p_2p_3}\right)}{4}$ and $\epsilon_c=\frac{-\left(1+\sqrt{-p_1p_2}-\sqrt{p_1p_3}-\sqrt{-p_2p_3}\right)}{4}$.

Again using 3.4[3], we have following result.

Theorem 2.8 If all p_i 's are of $4k+3$ form, then the various values of ε_i 's in the expression $\theta_1(x)$ are:

$$\epsilon_0=\frac{\phi(p_1p_2p_3)}{4},\ \epsilon_{p_1p_2}=-\frac{\phi(p_1p_2)}{4},\ \epsilon_{p_1p_3}=-\frac{\phi(p_1p_3)}{4},\ \epsilon_{p_2p_3}=-\frac{\phi(p_2p_3)}{4},\ \epsilon_{p_1}=\frac{\phi(p_1)\left(1+\sqrt{p_2p_3}\right)}{4},$$

$$\epsilon_{ap_1}=\frac{\phi(p_1)\left(1-\sqrt{p_2p_3}\right)}{4},\ \epsilon_{p_2}=\frac{\phi(p_2)\left(1+\sqrt{p_1p_3}\right)}{4},\ \epsilon_{bp_2}=\frac{\phi(p_2)\left(1-\sqrt{p_1p_3}\right)}{4},\ \epsilon_{p_3}=\frac{\phi(p_3)\left(1+\sqrt{p_1p_2}\right)}{4},$$

$$\epsilon_{cp_3}=\frac{\phi(p_3)\left(1-\sqrt{p_1p_2}\right)}{4},\ \epsilon_1=\frac{-\left(1+\sqrt{p_1p_2}+\sqrt{p_1p_3}+\sqrt{p_2p_3}\right)}{4},\ \epsilon_a=\frac{-\left(1+\sqrt{p_1p_2}-\sqrt{p_1p_3}-\sqrt{p_2p_3}\right)}{4},$$

$$\epsilon_b=\frac{-\left(1-\sqrt{p_1p_2}+\sqrt{p_1p_3}-\sqrt{p_2p_3}\right)}{4}\text{ and }\epsilon_c=\frac{-\left(1-\sqrt{p_1p_2}-\sqrt{p_1p_3}+\sqrt{p_2p_3}\right)}{4}.$$

Theorem 2.9 Let $p_1=4k+3$, $p_2=4k+1$ and $p_3=4k+3$. Further, let $-C_1^{p_1p_2p_3(l)}=C_a^{p_1p_2p_3(l)}$. Then

$$\sigma_0(\xi)=1,\ \sigma_{p_1p_2}(\xi)=-1,\ \sigma_{p_1p_3}(\xi)=-1,\ \sigma_{p_2p_3}(\xi)=-1,\ \sigma_{p_1}(\xi)=\left(\frac{1-\sqrt{-p_2p_3}}{2}\right),\ \sigma_{ap_1}(\xi)=\left(\frac{1+\sqrt{-p_2p_3}}{2}\right)$$

$$,\ \sigma_{p_2}(\xi)=\left(\frac{1+\sqrt{p_1p_3}}{2}\right),\ \sigma_{bp_2}(\xi)=\left(\frac{1-\sqrt{p_1p_3}}{2}\right),\ \sigma_{p_3}(\xi)=\left(\frac{1-\sqrt{-p_1p_2}}{2}\right),\ \sigma_{cp_3}(\xi)=\left(\frac{1+\sqrt{-p_1p_2}}{2}\right),$$

$$\sigma_1(\xi)=\frac{-\left(1-\sqrt{-p_1p_2}+\sqrt{p_1p_3}-\sqrt{-p_2p_3}\right)}{4},\ \sigma_a(\xi)=-\left(\frac{1-\sqrt{-p_1p_2}-\sqrt{p_1p_3}+\sqrt{-p_2p_3}}{4}\right),$$

$$\sigma_b(\xi)=-\left(\frac{1+\sqrt{-p_1p_2}-\sqrt{p_1p_3}-\sqrt{-p_2p_3}}{4}\right)\text{ and }\sigma_c(\xi)=-\left(\frac{1+\sqrt{-p_1p_2}+\sqrt{p_1p_3}+\sqrt{-p_2p_3}}{4}\right).$$

Proof. By Definition 2.2, in θ_1, $\epsilon_i=\sum_{s\in C_1^{p_1p_2p_3(l)}}\xi^{-si}=\sum_{s\in -C_1^{p_1p_2p_3(l)}}\xi^{si}=\frac{O\left(C_1^{p_1p_2p_3(l)}\right)}{O\left(C_i^{p_1p_2p_3(l)}\right)}\sigma_{-i}(\xi)$. Therefore,

$\sigma_i(\xi)=\frac{O\left(C_i^{p_1p_2p_3(l)}\right)}{O\left(C_1^{p_1p_2p_3(l)}\right)}\epsilon_{-i}$. By Observation 2.4(i) and by Theorem 2.7,

$$\sigma_0(\xi)=1,\ \sigma_{p_1p_2}(\xi)=\left(\frac{\phi(p_3)}{\frac{\phi(p_1p_2p_3)}{4}}\right)\left(-\frac{\phi(p_1p_2)}{4}\right)=-1,$$

$$\sigma_{p_1p_3}(\xi)=\left(\frac{\phi(p_2)}{\frac{\phi(p_1p_2p_3)}{4}}\right)\left(-\frac{\phi(p_1p_3)}{4}\right)=-1,$$

$$\sigma_{p_2p_3}(\xi)=\left(\frac{\phi(p_1)}{\frac{\phi(p_1p_2p_3)}{4}}\right)\left(-\frac{\phi(p_2p_3)}{4}\right)=-1,$$

$$\sigma_{p_1}(\xi)=\frac{\frac{\phi(p_2p_3)}{2}}{\frac{\phi(p_1p_2p_3)}{4}}\left(\frac{\phi(p_1)(1-\sqrt{-p_2p_3})}{4}\right)=\frac{1-\sqrt{-p_2p_3}}{2},$$

$$\sigma_{ap_1}(\xi)=\frac{\frac{\phi(p_2p_3)}{2}}{\frac{\phi(p_1p_2p_3)}{4}}\left(\frac{\phi(p_1)(1+\sqrt{-p_2p_3})}{4}\right)=\frac{1+\sqrt{-p_2p_3}}{2},$$

$$\sigma_{p_2}(\xi)=\frac{\frac{\phi(p_1p_3)}{2}}{\frac{\phi(p_1p_2p_3)}{4}}\left(\frac{\phi(p_2)(1+\sqrt{p_1p_3})}{4}\right)=\frac{1+\sqrt{p_1p_3}}{2},$$

$$\sigma_{bp_2}(\xi)=\frac{\frac{\phi(p_1p_3)}{2}}{\frac{\phi(p_1p_2p_3)}{4}}\left(\frac{\phi(p_2)(1-\sqrt{p_1p_3})}{4}\right)=\frac{1-\sqrt{p_1p_3}}{2},$$

$$\sigma_{p_3}(\xi)=\frac{\frac{\phi(p_1p_2)}{2}}{\frac{\phi(p_1p_2p_3)}{4}}\left(\frac{\phi(p_3)(1-\sqrt{-p_1p_2})}{4}\right)=\frac{1-\sqrt{-p_1p_2}}{2},$$

$$\sigma_{cp_3}(\xi)=\frac{\frac{\phi(p_1p_2)}{2}}{\frac{\phi(p_1p_2p_3)}{4}}\left(\frac{\phi(p_3)(1+\sqrt{-p_1p_2})}{4}\right)=\frac{1+\sqrt{-p_1p_2}}{2},$$

$$\sigma_1(\xi)=\epsilon_a=\frac{-\left(1-\sqrt{-p_1p_2}+\sqrt{p_1p_3}-\sqrt{-p_2p_3}\right)}{4},$$

$$\sigma_a(\xi)=\epsilon_1=-\left(\frac{1-\sqrt{-p_1p_2}-\sqrt{p_1p_3}+\sqrt{-p_2p_3}}{4}\right),$$

$$\sigma_b(\xi)=\epsilon_c=-\left(\frac{1+\sqrt{-p_1p_2}-\sqrt{p_1p_3}-\sqrt{-p_2p_3}}{4}\right) \text{ and}$$

$$\sigma_c(\xi)=\epsilon_b=-\left(\frac{1+\sqrt{-p_1p_2}+\sqrt{p_1p_3}+\sqrt{-p_2p_3}}{4}\right).\ \diamond$$

Corollary 2.10 Let $p_1=4k+3$, $p_2=4k+1$ and $p_3=4k+3$. If $-C_1^{p_1p_2p_3(l)}=C_b^{p_1p_2p_3(l)}$. Then $\sigma_0(\xi)=1$, $\sigma_{p_1p_2}(\xi)=-1$, $\sigma_{p_1p_3}(\xi)=-1$, $\sigma_{p_2p_3}(\xi)=-1$, $\sigma_{p_1}(\xi)=\left(\frac{1-\sqrt{-p_2p_3}}{2}\right)$, $\sigma_{ap_1}(\xi)=\left(\frac{1+\sqrt{-p_2p_3}}{2}\right)$,

$\sigma_{p_2}(\xi)=\left(\frac{1+\sqrt{p_1p_3}}{2}\right)$, $\sigma_{bp_2}(\xi)=\left(\frac{1-\sqrt{p_1p_3}}{2}\right)$, $\sigma_{p_3}(\xi)=\left(\frac{1-\sqrt{-p_1p_2}}{2}\right)$, $\sigma_{cp_3}(\xi)=\left(\frac{1+\sqrt{-p_1p_2}}{2}\right)$,
$\sigma_1(\xi)=-\left(\frac{1+\sqrt{-p_1p_2}+\sqrt{p_1p_3}+\sqrt{-p_2p_3}}{4}\right)$, $\sigma_a(\xi)=-\left(\frac{1+\sqrt{-p_1p_2}-\sqrt{p_1p_3}-\sqrt{-p_2p_3}}{4}\right)$,
$\sigma_b(\xi)=-\left(\frac{1-\sqrt{-p_1p_2}-\sqrt{p_1p_3}+\sqrt{-p_2p_3}}{4}\right)$ and $\sigma_c(\xi)=-\left(\frac{1-\sqrt{-p_1p_2}+\sqrt{p_1p_3}-\sqrt{-p_2p_3}}{4}\right)$.

Corollary 2.11 Let $p_1=4k+3$, $p_2=4k+1$ and $p_3=4k+3$. If $-C_1^{p_1p_2p_3(l)}=C_c^{p_1p_2p_3(l)}$. Then $\sigma_0(\xi)=1$,
$\sigma_{p_1p_2}(\xi)=-1$, $\sigma_{p_1p_3}(\xi)=-1$, $\sigma_{p_2p_3}(\xi)=-1$, $\sigma_{p_1}(\xi)=\left(\frac{1-\sqrt{-p_2p_3}}{2}\right)$, $\sigma_{ap_1}(\xi)=\left(\frac{1+\sqrt{-p_2p_3}}{2}\right)$,
$\sigma_{p_2}(\xi)=\left(\frac{1+\sqrt{p_1p_3}}{2}\right)$, $\sigma_{bp_2}(\xi)=\left(\frac{1-\sqrt{p_1p_3}}{2}\right)$, $\sigma_{p_3}(\xi)=\left(\frac{1-\sqrt{-p_1p_2}}{2}\right)$, $\sigma_{cp_3}(\xi)=\left(\frac{1+\sqrt{-p_1p_2}}{2}\right)$,
$\sigma_1(\xi)=-\left(\frac{1+\sqrt{-p_1p_2}-\sqrt{p_1p_3}-\sqrt{-p_2p_3}}{4}\right)$, $\sigma_a(\xi)=-\left(\frac{1+\sqrt{-p_1p_2}+\sqrt{p_1p_3}+\sqrt{-p_2p_3}}{4}\right)$,
$\sigma_b(\xi)=-\left(\frac{1-\sqrt{-p_1p_2}+\sqrt{p_1p_3}-\sqrt{-p_2p_3}}{4}\right)$ and $\sigma_c(\xi)=-\left(\frac{1-\sqrt{-p_1p_2}-\sqrt{p_1p_3}+\sqrt{-p_2p_3}}{4}\right)$.

Theorem 2.12 If all p_i 's are $4k+3$ form, then $\sigma_0(\xi)=1$, $\sigma_{p_1p_2}(\xi)=-1$, $\sigma_{p_1p_3}(\xi)=-1$, $\sigma_{p_2p_3}(\xi)=-1$,
$\sigma_{p_1}(\xi)=\frac{1+\sqrt{p_2p_3}}{2}$, $\sigma_{ap_1}(\xi)=\frac{1-\sqrt{p_2p_3}}{2}$, $\sigma_{p_2}(\xi)=\frac{1+\sqrt{p_1p_3}}{2}$, $\sigma_{bp_2}(\xi)=\frac{1-\sqrt{p_1p_3}}{2}$,
$\sigma_{p_3}(\xi)=\frac{1+\sqrt{p_1p_2}}{2}$, $\sigma_{cp_3}(\xi)=\frac{1-\sqrt{p_1p_2}}{2}$, $\sigma_1(\xi)=-\left(\frac{1+\sqrt{p_1p_2}+\sqrt{p_1p_3}+\sqrt{p_2p_3}}{4}\right)$,
$\sigma_a(\xi)=-\left(\frac{1+\sqrt{p_1p_2}-\sqrt{p_1p_3}-\sqrt{p_2p_3}}{4}\right)$, $\sigma_b(\xi)=-\left(\frac{1-\sqrt{p_1p_2}+\sqrt{p_1p_3}-\sqrt{p_2p_3}}{4}\right)$ and
$\sigma_c(\xi)=-\left(\frac{1-\sqrt{p_1p_2}-\sqrt{p_1p_3}+\sqrt{p_2p_3}}{4}\right)$.

Proof. In this case, by Observation 2.4(ii), $-C_i^{p_1p_2p_3(l)}=C_i^{p_1p_2p_3(l)}$, where i runs over each l -cyclotomic coset modulo $p_1p_2p_3$. By Definition 2.2, in θ_1,

$\epsilon_i=\sum_{s\in C_1^{p_1p_2p_3(l)}}\xi^{-si}=\sum_{s\in -C_1^{p_1p_2p_3(l)}}\xi^{si}=\sum_{s\in C_1^{p_1p_2p_3(l)}}\xi^{si}=\frac{O\left(C_1^{p_1p_2p_3(l)}\right)}{O\left(C_i^{p_1p_2p_3(l)}\right)}\sigma_i(\xi)$. Therefore,

$\sigma_i\left(\xi\right)=\frac{O\left(C_i^{p_1p_2p_3(l)}\right)}{O\left(C_1^{p_1p_2p_3(l)}\right)}\in_i$. Then, by Theorem 2.8,

$\sigma_0(\xi)=1$, $\sigma_{p_1p_2}(\xi)=\left(\frac{\phi(p_3)}{\frac{\phi(p_1p_2p_3)}{4}}\right)\left(-\frac{\phi(p_1p_2)}{4}\right)=-1$,

$$\sigma_{p_1p_3}(\xi)=\left(\frac{\phi(p_2)}{\frac{\phi(p_1p_2p_3)}{4}}\right)\left(-\frac{\phi(p_1p_3)}{4}\right)=-1,$$

$$\sigma_{p_2p_3}(\xi)=\left(\frac{\phi(p_1)}{\frac{\phi(p_1p_2p_3)}{4}}\right)\left(-\frac{\phi(p_2p_3)}{4}\right)=-1,$$

$$\sigma_{p_1}(\xi)=\frac{\frac{\phi(p_2p_3)}{2}}{\frac{\phi(p_1p_2p_3)}{4}}\left(\frac{\phi(p_1)(1+\sqrt{p_2p_3})}{4}\right)=\frac{1+\sqrt{p_2p_3}}{2},$$

$$\sigma_{ap_1}(\xi)=\frac{\frac{\phi(p_2p_3)}{2}}{\frac{\phi(p_1p_2p_3)}{4}}\left(\frac{\phi(p_1)(1-\sqrt{p_2p_3})}{4}\right)=\frac{1-\sqrt{p_2p_3}}{2},$$

$$\sigma_{p_2}(\xi)=\frac{\frac{\phi(p_1p_3)}{2}}{\frac{\phi(p_1p_2p_3)}{4}}\left(\frac{\phi(p_2)(1+\sqrt{p_1p_3})}{4}\right)=\frac{1+\sqrt{p_1p_3}}{2},$$

$$\sigma_{bp_2}(\xi)=\frac{\frac{\phi(p_1p_3)}{2}}{\frac{\phi(p_1p_2p_3)}{4}}\left(\frac{\phi(p_2)(1-\sqrt{p_1p_3})}{4}\right)=\frac{1-\sqrt{p_1p_3}}{2},$$

$$\sigma_{p_3}(\xi)=\frac{\frac{\phi(p_1p_2)}{2}}{\frac{\phi(p_1p_2p_3)}{4}}\left(\frac{\phi(p_3)(1+\sqrt{p_1p_2})}{4}\right)=\frac{1+\sqrt{p_1p_2}}{2},$$

$$\sigma_{cp_3}(\xi)=\frac{\frac{\phi(p_1p_2)}{2}}{\frac{\phi(p_1p_2p_3)}{4}}\left(\frac{\phi(p_3)(1-\sqrt{p_1p_2})}{4}\right)=\frac{1-\sqrt{p_1p_2}}{2},$$

$$\sigma_1(\xi)=\epsilon_1=-\frac{\frac{\phi(p_1p_2p_3)}{4}}{\frac{\phi(p_1p_2p_3)}{4}}\left(\frac{1+\sqrt{p_1p_2}+\sqrt{p_1p_3}+\sqrt{p_2p_3}}{4}\right)=-\left(\frac{1+\sqrt{p_1p_2}+\sqrt{p_1p_3}+\sqrt{p_2p_3}}{4}\right),$$

$$\sigma_a(\xi)=\epsilon_a=-\left(\frac{1+\sqrt{p_1p_2}-\sqrt{p_1p_3}-\sqrt{p_2p_3}}{4}\right),$$

$\sigma_b(\xi) = \epsilon_b = -\left(\frac{1-\sqrt{p_1 p_2}+\sqrt{p_1 p_3}-\sqrt{p_2 p_3}}{4}\right)$ and

$\sigma_c(\xi) = \epsilon_c = -\left(\frac{1-\sqrt{p_1 p_2}-\sqrt{p_1 p_3}+\sqrt{p_2 p_3}}{4}\right)$. ◊

2.13 Algorithm to compute the irreducible factors of $x^{p_1 p_2 p_3}-1$

We have following algorithm to compute the $\eta_s(x) = \prod_{s \in C_s^{p_1 p_2 p_3}(l)} \left(x - \xi^s\right)$.

Step 1. Compute $B = \{s_1 + s_2 + \ldots + s_k \vee s_j$ are distinct elements of $C_s^{p_1 p_2 p_3}(l)\}$

Step 2. Compute $t_{k,i}$, where $t_{k,i}$ are number of solutions of

$x_1 + x_2 + \ldots + x_k = i;$,I runs over each cyclotomic coset, in B.

Step 3. Compute $a_k = \sum t_{k,i}\sigma_i(\xi)$; i runs over each cyclotomic coset modulo $p_1 p_2 p_3$.

Step 4. The $\eta_s(x) = \sum_{k=0}^{O(C_s^{p_1 p_2 p_3(l)})} (-1)^k a_k x^{O(C_s^{p_1 p_2 p_3(l)})-k}$.

Step 5. Stop.

Example

Example In this example we find all the irreducible factors of $x^{105} - 1$ over F_{17} . The 14 distinct 17-cyclotomic cosets modulo 105 are $C_0^{105(17)}$, $C_1^{105(17)}$, $C_2^{105(17)}$, $C_{11}^{105(17)}$, $C_{22}^{105(17)}$, $C_3^{105(17)}$, $C_6^{105(17)}$, $C_5^{105(17)}$, $C_{10}^{105(17)}$, $C_7^{105(17)}$, $C_{49}^{105(17)}$, $C_{15}^{105(17)}$, $C_{21}^{105(17)}$ and $C_{35}^{105(17)}$. It is easy to see that

$\eta_0(x) = (x-1)$.

$\eta_{15}(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$,

$\eta_{21}(x) = x^4 + x^3 + x^2 + x + 1$, and

$\eta_{35}(x) = x^2 + x + 1$.

Computation of $\eta_3(x)$: The $\eta_3(x) = \sum_{i=0}^{12} (-1)^k a_k x^k$ where $a_k = \sum t_{k,i}\sigma_i(\gamma)$;

i runs over each cyclotomic coset modulo 105. By Theorem 2.5
$\sigma_0(\gamma) = 1, \sigma_1(\gamma) = 4, \sigma_2(\gamma) = 7, \sigma_{11}(\gamma) = 2, \sigma_{22}(\gamma) = 3, \sigma_3(\gamma) = 11, \sigma_6(\gamma) = 7, \sigma_5(\gamma) = 10, \sigma_{10}(\gamma) = 8, \sigma_7(\gamma) = 12, \sigma_{49}(\gamma) = 6, \sigma_{15}(\gamma) = -1, \sigma_{21}(\gamma) = -1$ and $\sigma_{35}(\gamma) = -1$
. It is easy to see that $a_0 = a_{12} = 1$.
Since

$t_{1,0} = 0, t_{1,1} = 0, t_{1,2} = 0, t_{1,11} = 0, t_{1,22} = 0, t_{1,3} = 1, t_{1,6} = 0, t_{1,5} = 0, t_{1,10} = 0, t_{1,7} = 0, t_{1,49} = 0, t_{1,15} = 0, t_{1,21} = 0, t_{1,35} = 0;\ a_1 = 11$,

$t_{2,0}=0, t_{2,1}=0, t_{2,2}=0, t_{1,11}=0, t_{2,22}=0, t_{2,3}=2, t_{2,6}=1, t_{2,5}=0, t_{2,10}=0, t_{2,7}=0, t_{2,49}=0, t_{2,15}=3, t_{2,21}=3, t_{2,35}=0$; $a_2=6$,

$t_{3,0}=0, t_{3,1}=0, t_{3,2}=0, t_{3,11}=0, t_{3,22}=0, t_{3,3}=6, t_{3,6}=7, t_{3,5}=0, t_{3,10}=0, t_{3,7}=0, t_{3,49}=0, t_{3,15}=6, t_{3,21}=7, t_{3,35}=0$; $a_3=0$,

$t_{4,0}=15, t_{4,1}=0, t_{4,2}=0, t_{4,11}=0, t_{4,22}=0, t_{4,3}=12, t_{4,6}=15, t_{4,5}=0, t_{4,10}=0, t_{4,7}=0, t_{4,49}=0, t_{4,15}=16, t_{4,21}=15, t_{4,35}=0$; $a_4=0$,

$t_{5,0}=24, t_{5,1}=0, t_{5,2}=0, t_{5,11}=0, t_{5,22}=0, t_{5,3}=22, t_{5,6}=25, t_{5,5}=0, t_{5,10}=0, t_{5,7}=0, t_{5,49}=0, t_{5,15}=20, t_{5,21}=21, t_{5,35}=0$; $a_5=9$,

$t_{6,0}=38, t_{6,1}=0, t_{6,2}=0, t_{6,11}=0, t_{6,22}=0, t_{6,3}=26, t_{6,6}=26, t_{6,5}=0, t_{6,10}=0, t_{6,7}=0, t_{6,49}=0, t_{6,15}=27, t_{6,21}=25, t_{6,35}=0$; $a_6=12$,

$t_{7,0}=24, t_{7,1}=0, t_{7,2}=0, t_{7,11}=0, t_{7,22}=0, t_{7,3}=25, t_{7,6}=22, t_{7,5}=0, t_{7,10}=0, t_{7,7}=0, t_{7,49}=0, t_{7,15}=20, t_{7,21}=21, t_{7,35}=0$; $a_7=4$,

$t_{8,0}=15, t_{8,1}=0, t_{8,2}=0, t_{8,11}=0, t_{8,22}=0, t_{8,3}=15, t_{8,6}=12, t_{8,5}=0, t_{8,10}=0, t_{8,7}=0, t_{8,49}=0, t_{8,15}=16, t_{8,21}=15, t_{8,35}=0$; $a_8=12$,

$t_{9,0}=0, t_{9,1}=0, t_{9,2}=0, t_{9,11}=0, t_{9,22}=0, t_{9,3}=7, t_{9,6}=6, t_{9,5}=0, t_{9,10}=0, t_{9,7}=0, t_{9,49}=0, t_{9,15}=6, t_{9,21}=7, t_{9,35}=0$; $a_9=4$,

$t_{10,0}=0, t_{10,1}=0, t_{10,2}=0, t_{10,11}=0, t_{10,22}=0, t_{10,3}=1, t_{10,6}=2, t_{10,5}=0, t_{10,10}=0, t_{10,7}=0, t_{10,49}=0, t_{10,15}=3, t_{10,21}=3, t_{10,35}=0$; $a_{10}=2$,

$t_{11,0}=0, t_{11,1}=0, t_{11,2}=0, t_{11,11}=0, t_{11,22}=0, t_{11,3}=0, t_{11,6}=1, t_{11,5}=0, t_{11,10}=0, t_{11,7}=0, t_{11,49}=0, t_{11,15}=0, t_{11,21}=0, t_{11,35}=0$; $a_{11}=7$,

Hence $\eta_3^{105}(x)=x^{12}+6x^{11}+6x^{10}+8x^7+12x^6+13x^5+12x^4+13x^3+2x^2+10x+1$.

Since the roots of η_6^{105} are reciprocal of roots of η_3^{105}, therefore,
$\eta_6^{105}(x)=x^{12}+10x^{11}+2x^{10}+13x^9+12x^8+13x^7+12x^6+8x^5+6x^2+6x+1$.

On similar steps we get

$\eta_5^{105}(x)=x^6+9x^5+10x^4+6x^3+10x^2+9x+1$,

$\eta_{10}^{105}(x)=x^6+7x^5+12x^4+4x^3+12x^2+7x+1$,

$\eta_7^{105}(x)=x^4+11x^3+15x^2+5x+1$,

$\eta_{49}^{105}(x)=x^4+5x^3+15x^2+11x+1$.

We now compute $\eta_1^{105}(x)$. Clearly $a_0=1, a_1=4, a_{11}=3, a_{12}=1$

Since

$t_{2,0}=0, t_{2,1}=1, t_{2,2}=0, t_{2,11}=0, t_{2,22}=0, t_{2,3}=1, t_{2,6}=1, t_{2,5}=2, t_{2,10}=1, t_{2,7}=0, t_{2,49}=0, t_{2,15}=0, t_{2,21}=3, t_{2,35}=0$; $a_2=13$,

$t_{3,0}=0, t_{3,1}=2, t_{3,2}=1, t_{3,11}=3, t_{3,22}=5, t_{3,3}=1, t_{3,6}=1, t_{3,5}=4, t_{3,10}=2, t_{3,7}=3, t_{3,49}=0, t_{3,15}=0, t_{3,21}=4, t_{3,35}=0$; $a_3=6$,

$t_{4,0}=15, t_{4,1}=5, t_{4,2}=3, t_{4,11}=3, t_{4,22}=7, t_{4,3}=4, t_{4,6}=5, t_{4,5}=4, t_{4,10}=1, t_{4,7}=3, t_{4,49}=3, t_{4,15}=11, t_{4,21}=9, t_{4,35}=0$; $a_4=6$,

$t_{5,0}=12, t_{5,1}=14, t_{5,2}=11, t_{5,11}=4, t_{5,22}=9, t_{5,3}=4, t_{5,6}=5, t_{5,5}=10, t_{5,10}=6, t_{5,7}=3, t_{5,49}=9, t_{5,15}=4, t_{5,21}=9, t_{5,35}=6$; $a_5=2$,

$t_{6,0}=14, t_{6,1}=9, t_{6,2}=5, t_{6,11}=5, t_{6,22}=9, t_{6,3}=12, t_{6,6}=12, t_{6,5}=13, t_{6,10}=10, t_{6,7}=3, t_{6,49}=3, t_{6,15}=4, t_{6,21}=19, t_{6,35}=12$; $a_6=6$,

$t_{7,0}=12, t_{7,1}=9, t_{7,2}=4, t_{7,11}=11, t_{7,22}=14, t_{7,3}=5, t_{7,6}=4, t_{7,5}=10, t_{7,10}=6, t_{7,7}=9, t_{7,49}=3, t_{7,15}=4, t_{7,21}=9, t_{7,35}=6$; $a_7=2$,

$t_{8,0}=15, t_{8,1}=7, t_{8,2}=3, t_{8,11}=3, t_{8,22}=5, t_{8,3}=5, t_{8,6}=4, t_{8,5}=4, t_{8,10}=1, t_{8,7}=3, t_{8,49}=3, t_{8,15}=11, t_{8,21}=9, t_{8,35}=0$; $a_8=12$,

$t_{9,0}=0, t_{9,1}=5, t_{9,2}=3, t_{9,11}=1, t_{9,22}=2, t_{9,3}=1, t_{9,6}=1, t_{9,5}=4, t_{9,10}=2, t_{9,7}=0, t_{9,49}=3, t_{9,15}=0, t_{9,21}=4, t_{9,35}=0$; $a_9=1$,

$t_{10,0}=0, t_{10,1}=0, t_{10,2}=0, t_{10,11}=0, t_{10,22}=1, t_{10,3}=1, t_{10,6}=1, t_{10,5}=2, t_{10,10}=1, t_{10,7}=0, t_{10,49}=0, t_{10,15}=0, t_{10,21}=3, t_{10,35}=0$; $a_{10}=12$,

Hence

$\eta_1^{105}(x)=x^{12}+13x^{11}+13x^{10}+11x^9+6x^8+15x^7+6x^6+15x^5+12x^4+16x^3+12x^2+14x+1$.

Since the roots of η_{22}^{105} are reciprocal of roots of η_1^{105}, therefore,

$\eta_{22}^{105}(x)=x^{12}+14x^{11}+12x^{10}+16x^9+12x^8+15x^7+6x^6+15x^5+6x^4+11x^3+13x^2+13x+1$.
$\eta_{11}^{105}(x)=x^{12}+15x^{11}+9x^{10}+15x^9+12x^8+15x^7+8x^6+15x^5+6x^4+14x^3+14x^2+10x+1$.

Similarly, we have

$\eta_2^{105}(x)=x^{12}+10x^{11}+14x^{10}+14x^9+6x^8+15x^7+8x^6+15x^5+12x^4+15x^3+9x^2+15x+1$.

Hence

$x^{105}-1=(x^{12}+10x^{11}+14x^{10}+14x^9+6x^8+15x^7+8x^6+15x^5+12x^4+15x^3+9x^2+15x+1)$
$(x^{12}+15x^{11}+9x^{10}+15x^9+12x^8+15x^7+8x^6+15x^5+6x^4+14x^3+14x^2+10x+1)$
$(x^{12}+13x^{11}+13x^{10}+11x^9+6x^8+15x^7+6x^6+15x^5+12x^4+16x^3+12x^2+14x+1)$
$(x^{12}+14x^{11}+12x^{10}+16x^9+12x^8+15x^7+6x^6+15x^5+6x^4+11x^3+13x^2+13x+1)$
$(x^{12}+10x^{11}+2x^{10}+13x^9+12x^8+13x^7+12x^6+8x^5+6x^2+6x+1)$
$(x^{12}+6x^{11}+6x^{10}+8x^7+12x^6+13x^5+12x^4+13x^3+2x^2+10x+1)(x^6+x^5+x^4+x^3+x^2+x+1)$
$(x^6+9x^5+10x^4+6x^3+10x^2+9x+1)(x^6+7x^5+12x^4+4x^3+12x^2+7x+1), (x^4+x^3+x^2+x+1)$
$(x^4+11x^3+15x^2+5x+1)(x^4+5x^3+15x^2+11x+1). (x^2+x+1)(x-1)$.

References

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

[2]. B. Chen, L. Li and R. Tuerhong, Explicit factorization of $x^{2^m p^n}-1$ 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 $_m$, *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 $p^n q^m$, *Int. J. Inform. Coding Theo.***2** (2014) 191-217.

[7]. F. Li and X. Cao, Explicit Factorization of $x^{2^a p^b r^c}-1$ 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.