International Journal of Pure and Applied Mathematics
Volume 105 No. 2 2015, 143-152
ISSN: 1311-8080 (printed version); ISSN: 1314-3395 (on-line version)
url: http://www.ijpam.eu
doi: http://dx.doi.org/10.12732/ijpam.v105i2.2

EXPLICIT FACTORIZATION OF CYCLOTOMIC POLYNOMIALS OVER FINITE FIELDS II

Okram Ratnabala Devi[1] §, Thiyam Rojita Chanu[2]

[1,2]Mathematics Department
Manipur University
Imphal, 795003, Manipur, INDIA

Abstract: Here, we make an attempt to study the explicit factorization of 2^n.7-th cyclotomic polynomials over finite field $\mathbb{F}_q$ when $q \equiv 3(\text{mod } 4)$ into a product of distinct monic irreducible polynomials, where q is a power of an odd prime which is relatively prime to 7.

AMS Subject Classification: 11T06, 11T55, 12Y05
Key Words: factorization, cyclotomic polynomials, finite fields, irreducible polynomials

1. Introduction

Let θ denote a primitive n^{th} root of unity. The n^{th} cyclotomic polynomial $Q_n(x)$ is defined as

$$Q_n(x) = \prod_{0<i\leq n,\ (i,n)=1} (x - \theta^i).$$

Clearly the degree of $Q_n(x)$ is $\varphi(n)$, where $\varphi(n)$ denotes the Euler's phi function.

Let q be a power of an odd prime p. Factorization of cyclotomic polynomials over finite fields have been studied extensively by many authors. For example, explicit factorization of $Q_{2^n}(x)$ into a product of irreducible polynomials over

Received: June 4, 2015

§Correspondence author

$\mathbb{F}_q$ are given in [5] when $q \equiv 1(mod\ 4)$ and in [1] for $q \equiv 3(mod\ 4)$. Fitzgerald and Yucas (see [6]) have studied the explicit factorization of $Q_{2^n.r}(x)$, where r is a prime and $q \equiv \pm 1(mod\ r)$ over $\mathbb{F}_q$. Liping Wang and Qiang Wang (see [3]) also studied the explicit factorization of $Q_{2^n.5}(x)$ over finite fields. The factorization of $Q_{2^n.7}(x)$ over $\mathbb{F}_q$ when $q \equiv 1(mod\ 4)$ is given in [4]. There are a number of applications on this topic. Some of the computer algebra systems use factorization of cyclotomic polynomial over finite fields for computing irreducible factors of any polynomial over finite fields.

In this paper, we study how the cyclotomic polynomial $Q_{2^n.7}(x)$ splits over finite field $\mathbb{F}_q$, q being a power of an odd prime relatively prime to 7 and also congruent to 3 modulo 4.

2. Preliminary Results

We shall begin with the following lemmata from [3] and [5] which will be used in developing the main results.

Lemma 1. Let $f_1(x)$,..., $f_N(x)$ be all distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree m and order e and let $t \geq 2$ be an integer whose prime factors divide e but not $(q^m - 1)/e$. Assume also that $q^m \equiv 1(mod\ 4)$ if $t \equiv 0(mod\ 4)$. Then $f_1(x^t)$,..., $f_N(x^t)$ are all distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree mt and order et.

Lemma 2. If (q, n)=1 , then $Q_n(x)$ factors into $\varphi(n)/d$ distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of the same degree d where d is the least positive integer such that $q^d \equiv 1(mod\ n)$.

It may be noted from Guerrier's theorem (see [7]) that if p divides n, then the irreducible factors of $Q_n(x)$ are repeated. Also, from [2] we see that $Q_n(\alpha)$=0 for some α in a field with characteristics p only when $n = p^e.k$ where k is the order of α modulo p. In this paper we will use some symbols with their significant meaning as given below. Let $\upsilon_2(k)$ denotes the highest power of 2 dividing k and $L_i = \upsilon_2(q^i - 1)$ for $i \geq 1$. In particular, let $L := L_{\varphi(r)} = \upsilon_2(q^{\varphi(r)} - 1)$, the highest power of 2 dividing $(q^{\varphi(r)} - 1)$ with $\varphi(r)$ the Euler's phi function. Let $\Omega(k)$ denote the set of primitive k^{th} roots of unity.

Lemma 3. Let $q = p^n$ be a power of an odd prime p. Let $r \geq 3$ be any odd number such that $(r, q) = 1$ and let $L := L_{\varphi(r)} = \upsilon_2(q^{\varphi(r)} - 1)$ the highest power of 2 dividing $(q^{\varphi(r)} - 1)$ with $\varphi(r)$ the Euler's phi function. For any $n \geq L$ and any irreducible factor $f(x)$ of $Q_{2^L.r}(x)$ over $\mathbb{F}_q$, $f(x^{2^{n-L}})$ is also irreducible over $\mathbb{F}_q$. Moreover, all irreducible factors of $Q_{2^L.r}(x)$ are obtained in this way.

3. Main Results

When we study the factorization of the cyclotomic polynomial $Q_{2^n.7}(x)$ over $\mathbb{F}_q$ when $q \equiv 3(mod\ 4)$, we need to consider six different cases depending on the values of q.

First of all, we consider the cases for $q \equiv \pm 1(mod\ 7)$ and $q \equiv 3(mod\ 4)$ i.e. $q \equiv 15(mod\ 28)$ or $q \equiv 27(mod\ 28)$, we get $L_1 = 1$, $L = 3 + \upsilon_2(7k+4)$ or $L = 3 + \upsilon_2(k+1)$, respectively for some k. We obtain the irreducible factors as linear, quadratic or a power of 2.

Theorem 4. *Let $q \equiv 1(mod\ 7)$ and $q \equiv 3(mod\ 4)$. Then we have the following factorization of $Q_{2^n.7}(x)$ over $\mathbb{F}_q$.*

(i) For $0 \leq n \leq 2$, we have

$$Q_7(x) = \prod_{\omega \in \Omega(7)} (x - \omega), \qquad Q_{2.7}(x) = \prod_{\omega \in \Omega(7)} (x + \omega),$$

$$Q_{2^2.7}(x) = \prod_{\omega \in \Omega(7)} (x^2 + \omega).$$

(ii) If $3 \leq n \leq L-1$, then

$$Q_{2^n.7}(x) = \prod_{\omega \in \Omega(7)} \prod_{\rho_n \in \Omega(2^n)} (x^2 - (\rho_n + \rho_n^{-1})\omega x + \omega^2).$$

(iii) If $n \geq L = L_6$, then

$$Q_{2^n.7}(x) = \prod_{\omega \in \Omega(7)} \prod_{\rho_L \in \Omega(2^L)} (x^{2^{n-L+1}} - (\rho_L - \rho_L^{-1})\omega x^{2^{n-L}} - \omega^2).$$

Proof. As $q \equiv 1(mod\ 7)$, we have $Q_7(x) = \prod_{\omega \in \Omega(7)}(x - \omega)$, $Q_{2.7}(x) = Q_7(-x) = \prod_{\omega \in \Omega(7)}(x + \omega)$. Also $x^2 + \omega$ is irreducible in $\mathbb{F}_q$ as -1 is a non square in $\mathbb{F}_q$. Therefore $Q_{2^2.7}(x) = \prod_{\omega \in \Omega(7)}(x^2 + \omega)$. Now $Q_{2^3.7}(x) = \prod_{\omega \in \Omega(7)}(x^4 + \omega)$. Then as $q^2 \equiv 1(mod\ 2^3.7)$, by lemma 2, each irreducible factor must have degree 2. So, let $(x^4 + \omega) = (x^2 + ax + b)(x^2 + cx + d)$ where $a, b, c, d \in \mathbb{F}_q$. Equating the coefficients we have $a = -c, b + d - c^2 = 0, (b - d)c = 0$ and $bd = \omega$. As $\omega^7 = 1$, let $\omega = \nu^6$ where $\nu = \omega^{-1}$. Moreover, -1 is a non square in this case. So, there are only two possibilities i.e. either $b = d = \nu^3$, $c^2 = 2$ if 2 is a square or $b = d = -\nu^3$, $c^2 = -2$ if -2 is a square. Also, in this case we can write $q \equiv 4k + 7(mod\ 8)$. So, when k is even, $q \equiv 7(mod\ 8)$ otherwise $q \equiv 3(mod\ 8)$.

However, $q \equiv 7(mod\ 8)$ implies that 2 is a square in $\mathbb{F}_q$. Similarly, -2 is a square in $\mathbb{F}_q$ if $q \equiv 3(mod\ 8)$. Also ω ranges over $\Omega(7)$ implies that ν ranges over $\Omega(7)$. Hence, we can write

$$Q_{2^3.7}(x) = \begin{cases} \prod_{\omega\in\Omega(7)} \prod_{c^2=-2}(x^2 + c\omega x - \omega^2) & \text{if } k \text{ is odd,} \\ \prod_{\omega\in\Omega(7)} \prod_{c^2=2}(x^2 + c\omega x + \omega^2) & \text{if } k \text{ is even.} \end{cases}$$

When k=odd, then L=3 and hence lemma 3 gives the rest of the proof of the theorem. If k=even, then L >3. For $4 \leq n \leq L-1$, ${\rho_n}^{q+1}$ =1 for any $\rho_n \in \Omega(2^n)$ which implies that $(\rho_n + {\rho_n}^{-1}) \in \mathbb{F}_q$. In particular $\rho_2 + {\rho_2}^{-1}$=0 and $(\pm(\rho_3 + {\rho_3}^{-1}))^2$=2.

Therefore

$$Q_{2^3.7}(x) = \prod_{\omega\in\Omega(7)} \prod_{\rho_3\in\Omega(2^3)} (x^2 - (\rho_3 + \rho_3^{-1})\omega x + \omega^2).$$

Let $\omega = u^2$. Then, one can easily show that for $4 \leq n \leq L-1$

$$x^4 + (\rho_{n-1} + {\rho_{n-1}}^{-1})u^2x^2 + u^4 = (x^2 - (\rho_n + {\rho_n}^{-1})ux + u^2)(x^2 + (\rho_n + {\rho_n}^{-1})ux + u^2)$$

Therefore, for k even and $4 \leq n \leq L-1$, we get

$$Q_{2^n.7}(x) = \prod_{\omega\in\Omega(7)} \prod_{\rho_n\in\Omega(2^n)} (x^2 - (\rho_n + \rho_n^{-1})\omega x + \omega^2).$$

Finally for $n = L$, ${\rho_L}^{q+1} = -1$ which implies that $(\rho_L - {\rho_L}^{-1}) \in \mathbb{F}_q$. Also $x^4 - (\rho_{L-1} + {\rho_{L-1}}^{-1})u^2x^2 + u^4 = (x^2 - (\rho_L - {\rho_L}^{-1})ux - u^2)(x^2 + (\rho_L - {\rho_L}^{-1})ux - u^2)$.Hence, $Q_{2^L.7}(x) = \prod_{\omega\in\Omega(7)} \prod_{\rho_L\in\Omega(2^L)}(x^2 - (\rho_L - \rho_L^{-1})\omega x - \omega^2)$. Combining lemma 3 and $Q_{2^n.7}(x) = Q_{2^L.7}(x^{2^{n-L}})$ together yields the rest of the proof. □

Theorem 5. *Let $q \equiv -1(mod\ 7)$ and $q \equiv 3(mod\ 4)$ and $\omega \in \Omega(7)$. Then we have the following factorization of $Q_{2^n.7}(x)$ over $\mathbb{F}_q$.*

(i) For n = 0 and 1, we have

$$Q_7(x) = \prod_{j=1,2,3} (x^2 - (\omega^j + \omega^{-j})x + 1), Q_{2.7}(x) = \prod_{j=1,2,3} (x^2 + (\omega^j + \omega^{-j})x + 1)$$

(ii) If n=2, then

$$Q_{2^2.7}(x) = \prod_{\rho_2\in\Omega(2^2)} \prod_{\substack{a_2=\rho_2\omega^j + (\rho_2\omega^j)^{-1} \\ j=1,2,3}} (x^2 + a_2x + 1)$$

(iii) If $3 \leq n \leq L-1$, *then*

$$Q_{2^n.7}(x) = \prod_{\rho_n \in \Omega(2^n)} \prod_{\substack{a_n = \rho_2\rho_n\omega^j + (\rho_2\rho_n\omega^j)^{-1} \\ j=1,2,3}} (x^2 + a_n x + 1)$$

(iv) If $n \geq L = L_6$, *then*

$$Q_{2^n.7}(x) = \prod_{\rho_L \in \Omega(2^L)} \prod_{\substack{a_L = \rho_2\rho_L\omega^j - (\rho_2\rho_L\omega^j)^{-1} \\ j=1,2,3}} (x^{2^{n-L+1}} + a_L x^{2^{n-L}} - 1)$$

Proof. For $0 \leq n \leq L-1$, $q^2 \equiv 1 (mod\ 2^n.7)$. Then, lemma 2 implies that $Q_{2^n.7}(x)$ factors into $\varphi(2^n.7)/2$ distinct irreducible polynomials over $\mathbb{F}_q$. Also $\omega^{q+1} = 1$ implies that $\omega^j + \omega^{-j} \in \mathbb{F}_q$ for $j = 1, 2, 3$. Hence, we have $Q_7(x) = \prod_{j=1,2,3}(x^2 - (\omega^j + \omega^{-j})x + 1)$, $Q_{2.7}(x) = \prod_{j=1,2,3}(x^2 + (\omega^j + \omega^{-j})x + 1)$. Now $Q_{2^2.7}(x) = \prod_{j=1,2,3}(x^4 + (\omega^j + \omega^{-j})x^2 + 1)$. Set $a_1 = \omega^j + \omega^{-j}$ for $j = 1, 2, 3$ then $\rho_2\omega^j + (\rho_2\omega^j)^{-1} \in \mathbb{F}_q$ as $(\rho_2\omega^j)^{q+1} = 1$. Also we can write $x^4 + a_1x^2 + 1 = (x^2 + a_2x + 1)(x^2 - a_2x + 1)$ where $a_2 = \rho_2(\omega^{4j} - \omega^{-4j}) = \rho_2\omega^{4j} + (\rho_2\omega^{4j})^{-1} \in \mathbb{F}_q$.

Therefore

$$Q_{2^2.7}(x) = \prod_{\rho_2 \in \Omega(2^2)} \prod_{\substack{a_2 = \rho_2(\omega^j - \omega^{-j}) \\ j=1,2,3}} (x^2 + a_2 x + 1)$$

$$= \prod_{\rho_2 \in \Omega(2^2)} \prod_{\substack{a_2 = \rho_2\omega^j + (\rho_2\omega^j)^{-1} \\ j=1,2,3}} (x^2 + a_2 x + 1)$$

For k=even, L=3. Let $a_3 = \rho_2\rho_3\omega^{4j} - (\rho_2\rho_3\omega^{4j})^{-1}$. Then, $a_3 \in \mathbb{F}_q$ as ${\rho_2}^{q+1} = 1$, ${\rho_3}^{q+1} = -1$ and $\omega^{(q+1)j} = 1$. Moreover $(x^2 + a_3x - 1)(x^2 - a_3x - 1) = x^4 + a_2x^2 + 1$ where $a_3^2 = -\rho_2\omega^j - (\rho_2^{-1}\omega^{-j}) - 2 = -a_2 - 2$.

Therefore

$$Q_{2^3.7}(x) = \prod_{\rho_3 \in \Omega(2^3)} \prod_{\substack{a_3 = \rho_2\rho_3\omega^j - (\rho_2\rho_3\omega^j)^{-1} \\ j=1,2,3}} (x^2 + a_3 x - 1).$$

For $n > L$, lemma 3 gives the rest of the proof of the theorem for k=even. Let k=odd. Then $L_3 > 3$. Suppose $3 \leq n \leq L-1$ and work inductively. Let $a_n = \rho_2\rho_n\omega^j + (\rho_2\rho_n\omega^j)^{-1}$. Since ${\rho_n}^{q+1} = 1$, then $(\rho_2\rho_n\omega^j)^{q+1} = 1$ for $3 \leq n \leq L-1$. Hence $a_n \in \mathbb{F}_q$. Moreover $x^4 + a_2x^2 + 1 = (x^2 + a_3x + 1)(x^2 - a_3x + 1)$ where $a_2 = 2 - {a_3}^2$.

Therefore

$$Q_{2^3.7}(x) = \prod_{\rho_3 \in \Omega(2^3)} \prod_{\substack{a_3 = \rho_2\rho_3\omega^j + (\rho_2\rho_3\omega^j)^{-1} \\ j=1,2,3}} (x^2 + a_3 x + 1).$$

Also we note that ρ_{n-1} ranges over $\Omega(2^{n-1})$ iff $\rho_2\rho_{n-1}$ ranges over $\Omega(2^{n-1})$ for $n \geq 4$. For $n \geq 4$, $(\rho_2\rho_{n-1})^{2^{n-1}} = (\rho_{n-1})^{2^{n-1}} = 1$ and $(\rho_2\rho_{n-1})^{2^{n-2}} = (\rho_{n-1})^{2^{n-2}} \neq 1$. This simplifies that

$$Q_{2^3.7}(x) = \prod_{\rho_3 \in \Omega(2^3)} \prod_{\substack{a_3 = \rho_3\omega^j + (\rho_3\omega^j)^{-1} \\ j=1,2,3}} (x^2 + a_3 x + 1).$$

Now we can see that $2 - {a_n}^2 = \rho_{n-1}\omega^j + (\rho_{n-1}\omega^j)^{-1}$ which is one of the a_{n-1}'s as ρ_{n-1} ranges over $\Omega(2^{n-1})$ for $n \geq 4$.

Therefore

$$Q_{2^n.7}(x) = Q_{2^{n-1}.7}(x^2) = \prod_{\rho_{n-1} \in \Omega(2^{n-1})} \prod_{\substack{a_{n-1} = \rho_{n-1}\omega^j + (\rho_{n-1}\omega^j)^{-1} \\ j=1,2,3}} (x^4 + a_{n-1}x^2 + 1)$$

$$= \prod_{\rho_n \in \Omega(2^n)} \prod_{\substack{a_n = \rho_2\rho_n\omega^j + (\rho_2\rho_n\omega^j)^{-1} \\ j=1,2,3}} (x^2 + a_n x + 1)$$

$$= \prod_{\rho_n \in \Omega(2^n)} \prod_{\substack{a_n = \rho_n\omega^j + (\rho_n\omega^j)^{-1} \\ j=1,2,3}} (x^2 + a_n x + 1).$$

For $n = L$, we have ${\rho_L}^2 = \rho_{L-1}$ and $a_L = \rho_2\rho_L\omega^{4j} - (\rho_2\rho_L\omega^{4j})^{-1}$. As ${\rho_2}^{q+1} = 1$ and $\omega^{(q+1)j} = 1$, $a_L \in \mathbb{F}_q$. Also we have ${a_L}^2 = -a_{L-1} - 2$ for a different choice of ρ_{L-1}. Hence

$$x^4 + a_{L-1}x^2 + 1 = (x^2 + a_L x - 1)(x^2 - a_L x - 1).$$

Hence

$$Q_{2^L.7}(x) = \prod_{\rho_L \in \Omega(2^L)} \prod_{\substack{a_L = \rho_2\rho_L\omega^j - (\rho_2\rho_L\omega^j)^{-1} \\ j=1,2,3}} (x^2 + a_L x - 1)$$

For $n > L$, lemma 3 and $Q_{2^n.7}(x) = Q_{2^L.7}(x^{2^{n-L}})$ together gives the rest of the proof. □

Further, we consider the cases when $q \equiv 2,\text{-}3(\text{mod } 7)$ and $q \equiv 3(\text{mod } 4)$ i.e. $q \equiv 23(\text{mod } 28)$ and $q \equiv 11(\text{mod } 28)$. Then, we get $L = 3 + \upsilon_2(7k+6)$ or $L = 3 + \upsilon_2(7k+3)$ for some k according as $q \equiv 23(\text{mod } 28)$ or $q \equiv 11(\text{mod } 28)$ and $L_1 = 1$. In these cases, we find that the degree of the irreducible factors are of the form 3.2^m for some m.

Theorem 6. *Let $q \equiv 2, -3(mod\ 7)$ and $q \equiv 3(mod\ 4)$ and $\omega \in \Omega(7)$. Then we have the following factorization of $Q_{2^n.7}(x)$ over $\mathbb{F}_q$.*

(i) For $n = 0$,1 and 2, we have

$$Q_7(x) = \prod_{\substack{j=2k-1 \\ k=1,2}} (x^3 - (\omega^j + \omega^{2j} + \omega^{4j})x^2 + (\omega^{3j} + \omega^{5j} + \omega^{6j})x - 1)$$

$$Q_{2.7}(x) = \prod_{\substack{j=2k-1 \\ k=1,2}} (x^3 + (\omega^j + \omega^{2j} + \omega^{4j})x^2 + (\omega^{3j} + \omega^{5j} + \omega^{6j})x + 1)$$

$$Q_{2^2.7}(x) = \prod_{\substack{j=2k-1 \\ k=1,2}} (x^6 + (\omega^j + \omega^{2j} + \omega^{4j})x^4 + (\omega^{3j} + \omega^{5j} + \omega^{6j})x^2 + 1)$$

(ii) If $3 \leq n \leq L-1$, then

$$Q_{2^n.7}(x) = \prod_{a_n,b_n,c_n,d_n,e_n} (x^6 + a_n x^5 + b_n x^4 + c_n x^3 + d_n x^2 + e_n x - 1)$$

where a_n, b_n, c_n, d_n, e_n satisfy the following non-linear recurrence relations $2b_n - a_n^2 = a_{n-1}, 2d_n - 2a_n c_n + b_n^2 = b_{n-1}, 2 - 2a_n e_n + 2b_n d_n - c_n^2 = c_{n-1}, 2b_n - 2e_n c_n + d_n^2 = d_{n-1}$ and $2d_n - e_n^2 = e_{n-1}$ with initial values $(a_2, b_2, c_2, d_2, e_2) = (0, (\omega + \omega^2 + \omega^4), 0, (\omega^3 + \omega^5 + \omega^6), 0)$ and $(a_2, b_2, c_2, d_2, e_2) = (0, (\omega^3 + \omega^5 + \omega^6), 0, (\omega + \omega^2 + \omega^4), 0)$.

(iii) If $n \geq L = L_6$, then

$$Q_{2^n.7}(x) = \prod_{a_L,b_L,c_L,d_L,e_L} (x^{3.2^{n-L+1}} + a_L x^{5.2^{n-L}} +$$

$$b_L x^{2^{n-L+2}} + c_L x^{3.2^{n-L}} + d_L x^{2^{n-L+1}} + e_L x^{2^{n-L}} - 1)$$

where a_L, b_L, c_L, d_L, e_L satisfy the following system of non-linear recurrence relations $2b_L - a_L^2 = a_{L-1}, 2d_L - 2a_L c_L + b_L^2 = b_{L-1}, -2 - 2a_L e_L + 2b_L d_L - c_L^2 = c_{L-1}, -2b_L - 2e_L c_L + d_L^2 = d_{L-1}$ and $-2d_L - e_L^2 = e_{L-1}$ for each five tuple of $a_{L-1}, b_{L-1}, c_{L-1}, d_{L-1}, e_{L-1}$ obtained in (ii).

Proof. Let $\omega \in \Omega(7)$ then $\omega \notin \mathbb{F}_q$. And it is clear that $(\omega+\omega^2+\omega^4), (\omega^3+\omega^5+\omega^6) \in \mathbb{F}_q$. For $0 \leq n \leq L-1$, $q^3 \equiv 1(mod 2^n.7)$. Hence we have $Q_7(x) = \prod_{j=2k-1,\ k=1,2}(x^3-(\omega^j+\omega^{2j}+\omega^{4j})x^2+(\omega^{3j}+\omega^{5j}+\omega^{6j})x-1)$ and $Q_{2.7}(x) = \prod_{j=2k-1,\ k=1,2}(x^3+(\omega^j+\omega^{2j}+\omega^{4j})x^2+(\omega^{3j}+\omega^{5j}+\omega^{6j})x+1)$. By lemma 1, the factors for

$$Q_{2^2.7}(x) = \prod_{\substack{j=2k-1\\ k=1,2}} (x^6+(\omega^j+\omega^{2j}+\omega^{4j})x^4+(\omega^{3j}+\omega^{5j}+\omega^{6j})x^2+1)$$

are irreducible over $\mathbb{F}_q$. For $3 \leq n \leq L-1$, by lemma 2 each irreducible factor must have degree 6 and also we note that $Q_{2^n.7}(x) = Q_{2^{n-1}.7}(x^2)$. Therefore we need to consider only the following factorization $(x^{12}+a_{n-1}x^{10}+b_{n-1}x^8+c_{n-1}x^6+d_{n-1}x^4+e_{n-1}x^2+1) = (x^6+a_5x^5+a_4x^4+a_3x^3+a_2x^2+a_1x+a_0)(x^6+b_5x^5+b_4x^4+b_3x^3+b_2x^2+b_1x+b_0)$. Since all the roots of an irreducible factor are the conjugates of a primitive $2^n.7$-th root of unity, a_0 and b_0 are of the form $\beta^{(1+q+q^2+q^3+q^4+q^5)}$ for some primitive $2^n.7$-th root of unity β. We note that $2^n.7 \mid (1+q+q^2+q^3+q^4+q^5)$ for $3 \leq n \leq L-1$. So, $a_0 = b_0 = 1$ and comparing the above equation we get $a_1 = -b_1$, $a_5 = -b_5$. Also we observe that $a_2 = b_2$, $a_3 = -b_3$ and $a_4 = b_4$. Therefore, $(x^{12}+a_{n-1}x^{10}+b_{n-1}x^8+c_{n-1}x^6+d_{n-1}x^4+e_{n-1}x^2+1) = (x^6+a_nx^5+b_nx^4+c_nx^3+d_nx^2+e_nx+1)(x^6-a_nx^5+b_nx^4-c_nx^3+d_nx^2-e_nx+1)$ satisfying the following non linear recurrence relations $2b_n-a_n^2 = a_{n-1}, 2d_n-2a_nc_n+b_n^2 = b_{n-1}, 2-2a_ne_n+2b_nd_n-c_n^2 = c_{n-1}, 2b_n-2e_nc_n+d_n^2 = d_{n-1}$ and $2d_n-e_n^2 = e_{n-1}$. Finally for $n = L$, $2^L.7 \nmid (1+q+q^2+q^3+q^4+q^5)$ and $2^{L-1}.7 \mid (1+q+q^2+q^3+q^4+q^5)$. So, $a_0 = b_0 = -1$. Hence, we have

$$Q_{2^L.7}(x) = \prod_{a_L,b_L,c_L,d_L,e_L} (x^6+a_Lx^5+b_Lx^4+c_Lx^3+d_Lx^2+e_Lx-1)$$

satisfying $2b_L-a_L^2 = a_{L-1}, 2d_L-2a_Lc_L+b_L^2 = b_{L-1}, -2-2a_Le_L+2b_Ld_L-c_L^2 = c_{L-1}, -2b_L-2e_Lc_L+d_L^2 = d_{L-1}$ and $-2d_L-e_L^2 = e_{L-1}$ Then, for $n > L$ the result follows from lemma 3 and $Q_{2^n.7}(x) = Q_{2^L.7}(x^{2^{n-L}})$. □

Lastly, we consider the cases when $q \equiv$ -2,3(mod 7) and $q \equiv 3$(mod 4) i.e. $q \equiv 19$(mod 28) or $q \equiv 3$(mod 28). Then, we get $L = 3+\upsilon_2(7k+5)$ or $L = 3+\upsilon_2(7k+1)$ respectively for some k and $L_1 = 1$. For these cases also, we obtain that the degree of the irreducible factors are of the form 3.2^m for some m.

Theorem 7. *Let $q \equiv -2, 3(mod\ 7)$ and $q \equiv 3(mod\ 4)$, then we have the following factorization of $Q_{2^n.7}(x)$ over $\mathbb{F}_q$.*

(i) If $0 \leq n \leq 1$, *then*

$$Q_{2^n.7}(x) = \prod_{\rho_n \in \Omega(2^n)} (x^6 + \rho_n x^5 + \rho_n^2 x^4 + \rho_n^3 x^3 + \rho_n^4 x^2 + \rho_n^5 x + \rho_n^6)$$

(ii) If $2 \leq n \leq L_6 - 1$, *then*

$$Q_{2^n.7}(x) = \prod_{a_n, b_n, c_n, d_n, e_n} (x^6 + a_n x^5 + b_n x^4 + c_n x^3 + d_n x^2 + e_n x + 1)$$

where a_n, b_n, c_n, d_n, e_n *satisfy the following non-linear recurrence relations* $2b_n - a_n^2 = a_{n-1}, 2d_n - 2a_n c_n + b_n^2 = b_{n-1}, 2 - 2a_n e_n + 2b_n d_n - c_n^2 = c_{n-1}, 2b_n - 2e_n c_n + d_n^2 = d_{n-1}$ *and* $2d_n - e_n^2 = e_{n-1}$ *with initial values* $a_1 = -1, b_1 = 1, c_1 = -1, d_1 = 1, e_1 = -1$.

(iii) If $n \geq L = L_6$, *then*

$$Q_{2^n.7}(x) = \prod_{a_L, b_L, c_L, d_L, e_L} (x^{3.2^{n-L+1}} + a_L x^{5.2^{n-L}} + b_L x^{2^{n-L+2}} + c_L x^{3.2^{n-L}} + d_L x^{2^{n-L+1}} + e_L x^{2^{n-L}} - 1)$$

where a_L, b_L, c_L, d_L, e_L *satisfy the following non-linear recurrence relations* $2b_L - a_L^2 = a_{L-1}, 2d_L - 2a_L c_L + b_L^2 = b_{L-1}, -2 - 2a_L e_L + 2b_L d_L - c_L^2 = c_{L-1}, -2b_L - 2e_L c_L + d_L^2 = d_{L-1}$ *and* $-2d_L - e_L^2 = e_{L-1}$ *for each five tuple of* $a_{L-1}, b_{L-1}, c_{L-1}, d_{L-1}, e_{L-1}$ *obtained in* (*ii*).

Proof. It is clear for $Q_7(x)$ and $Q_{2.7}(x)$. For $2 \leq n \leq L - 1$ and $n \geq L$, by proceeding the same process as in theorem 6, we obtain that the factors satisfy the recurrence relation of (ii) and (iii) respectively with initial values $a_1 = -1, b_1 = 1, c_1 = -1, d_1 = 1, e_1 = -1$. □

Now, as an illustration of some of our results, we provide the following tables of examples which we carried out the computation by using MATHEMATICA software. The coefficients (a_n, b_n) for quadratic, (a_n, b_n, c_n) for cubic and $(a_n, b_n, c_n, d_n, e_n, f_n)$ for factor having degree 6 of the irreducible factors of $Q_{2^n.7}(x)$ over $\mathbb{F}_q$ where q =83 and 67 for Theorem 5 and 6 respectively.

Example 1. Factorization of $Q_{2^n.7}(x)$ over $\mathbb{F}_q$ when $q = 83$.

n	1	2	3
(a_n, b_n)	(10,1)	(18,1),(30,1)	(4,-1)(7,-1),(32,-1),(14,-1)
	(15,1)	(32,1)(51,1)	(35,-1),(47,-1),(48,-1),(36,-1)
	(57,1)	(53,1),(65,1)	(76,-1),(79,-1),(51,-1),(69,-1)

Example 2. Factorization of $Q_{2^n.7}(x)$ over $\mathbb{F}_q$ when $q = 67$.

n	1	2	3
(a_n, b_n, c_n) for cubic or $(a_n, b_n, c_n, d_n, e_n, f_n)$ for having degree 6	(11,55,1) (55,11,1)	(0,11,0,55,0,1) (0,55,0,11,0,1)	(19,13,47,10,28,66) (28,57,47,54,19,66) (39,57,20,54,48,66) (48,13,20,10,39,66)

Acknowledgments

Authors are much thankful for the financial assistance provided by CSIR under SRF scheme.

References

[1] H. Meyn, Factorization of cyclotomic polynomials over finite fields, *Finite Fields Appl.,* **2** (1992), 439-442.

[2] K. Motose, On values of cyclotomic polynomials V, *Math. J. Okayama Univ.,* **45** (2003), 29-36.

[3] L. Wang, Q. Wang, On explicit factors of cyclotomic polynomials over finite fields, *Design Codes and Cryptography, Springer,* **3**, 1 (2012), 87-104.

[4] O.R. Devi , Th.R. Chanu, Explicit factorization of Cyclotomic polynomials over finite fields, *IJPAM,* **86**, 3 (2013), 585-592.

[5] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Application, Cambridge University Press, Cambridge (1997).

[6] R.W. Fitzgerald, J.L. Yucas, Explicit factorization of Cyclotomic and Dickson polynomials over finite fields, *Arithmetic of finite fields, Lecture Notes in Computer Science,* **4547** (2007), 1-10.

[7] W.J. Guerrier, The factorization of the cyclotomic polynomials mod p, *American Mathematical Monthly,* **75** (1968), 46.