EXPLICIT FACTORIZATION OF CYCLOTOMIC POLYNOMIALS OVER FINITE FIELDS

O. Ratnabala Devi¹ §, Th. Rojita Chanu²

^{1,2}Department of Mathematics
Manipur University
Imphal, 795003, Manipur, INDIA

Abstract: In this paper, we make an attempt to study the explicit factorization of 2^n -th cyclotomic polynomials over finite field $\mathbb{F}_q$ when $q \equiv 1 \pmod{4}$ into a product of distinct monic irreducible polynomials, where q is a power of an odd prime.

AMS Subject Classification: 11T06, 11T22, 12Y05

Key Words: cyclotomic polynomial, finite field, Dickson polynomial

1. Introduction

Let q be a power of an odd prime p . The n^{th} cyclotomic polynomial $Q_n(x)$ is defined as

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

where ω is the n^{th} root of unity.

Explicit factorization of the cyclotomic polynomial $Q_{2^n}(x)$ into a product of irreducible polynomials over $\mathbb{F}_q$ are given in [4] when $q \equiv 1 \pmod{4}$. The case for $q \equiv 3 \pmod{4}$ is done in [1] by Helmut Meyn. Fitzgerald and Yucas [5] have studied the explicit factorization of $Q_{2^n.r}(x)$, where r is a prime and $q \equiv \pm 1 \pmod{r}$ over $\mathbb{F}_q$ in order to obtain the explicit factorization of Dickson polynomial which results to the explicit factorization of $Q_{2^n.3}(x)$ and Dickson

Received: November 10, 2012

© 2013 Academic Publications, Ltd.
url: www.acadpubl.eu

§Correspondence author

polynomial $D_{2^n.3}(x)$ over $\mathbb{F}_q$. Recently, Liping Wang and Qiang Wang [3] have shown that all irreducible factors of cyclotomic polynomial can be obtained easily from irreducible factors of cyclotomic polynomial of small orders and also studied the explicit factorization of $2^n.5$ -th cyclotomic polynomial over finite fields which give rise to the construction of several classes of irreducible polynomial of degree 2^{n-2} with fewer than 5 terms.

In this paper, we study the factors of the cyclotomic polynomial $Q_{2^n.7}(x)$ over finite field $\mathbb{F}_q$ when $q \equiv \pm 1, \pm 2, \pm 3 \pmod{7}$ as an extension of [3] and [5].

2. Preliminary Notes

In this section, we mention some of the important results from [3] and [4] and produce these in the following lemmas for the sake of completeness.

Lemma 2.1. (see Theorem 3.35 in [4]) *Let $f_1(x), \dots, f_N(x)$ 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 $q^m \equiv 1 \pmod{4}$ if $t \equiv 0 \pmod{4}$. Then $f_1(x^t), \dots, f_N(x^t)$ are all distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of degree mt and order et .*

Lemma 2.2. (see Theorem 2.47 in [4]) *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 $q^d \equiv 1 \pmod{n}$.*

Here we note 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 $n = p^e \cdot k$ where k is the order of α . For the elementary properties of cyclotomic polynomials see chapter 2 of [4]. In this paper we will use some symbols with their significant meaning as given below. Let $v_2(k)$ denotes the highest power of 2 dividing k and $L_i = v_2(q^i - 1)$ for $i \geq 1$. In particular, let $L := L_{\varphi(r)} = v_2(q^{\varphi(r)} - 1)$, the highest power of 2 dividing $(q^{\varphi(r)} - 1)$ with $\varphi(r)$ the Euler's phi function. Let $\Omega(k)$ denote the primitive k^{th} root of unity.

Lemma 2.3. (see Theorem 2.2 in [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 $L := L_{\varphi(r)} = v_2(q^{\varphi(r)} - 1)$ 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 give the factors of the cyclotomic polynomial, we have to deal with six different cases depending on the values of q .

First of all, we consider the cases when $q \equiv \pm 1 \pmod{7}$ and $q \equiv 1 \pmod{4}$ i.e. $q \equiv 1 \pmod{28}$ and $q \equiv 13 \pmod{28}$. Then, we get $L_6 = L_1 + 1$ where $L_1 = 2 + v_2(7k)$ or $L_1 = 2 + v_2(7k + 3)$ respectively. We have the following two theorems for these cases.

Theorem 3.1. *Let $q \equiv 1 \pmod{28}$. Then we have the following factorization of $Q_{2^n,7}(x)$ over $\mathbb{F}_q$ as given below.*

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

$$Q_7(x) = \prod_{\omega \in \Omega(7)} (x - \omega), \quad Q_{2,7}(x) = \prod_{\omega \in \Omega(7)} (x + \omega)$$

(ii) If $2 \leq n \leq L_1$, then

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

(iii) If $n \geq L = L_1 + 1$, then

$$Q_{2^n,7}(x) = \prod_{\omega \in \Omega(7)} \prod_{\rho_{L_1} \in \Omega(2^{L_1})} (x^{2^{n-L_1}} - \omega \rho_{L_1}).$$

Proof. Same as in [5] □

Theorem 3.2. *Let $q \equiv 13 \pmod{28}$ and $\omega \in \Omega(7)$. Then we have the following factorization of $Q_{2^n,7}(x)$ over $\mathbb{F}_q$ as given below.*

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

$$Q_7(x) = \prod_{j=1,2,3} (x^2 - (\omega^j + \omega^{-j})x + 1), \quad Q_{2,7}(x) = \prod_{j=1,2,3} (x^2 + (\omega^j + \omega^{-j})x + 1)$$

(ii) If $2 \leq n \leq L_1$, then

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

(iii) If $n \geq L = L_1 + 1$, then

$$Q_{2^n.7}(x) = \prod_{\rho_{L_1} \in \Omega(2^{L_1})} \prod_{a_L^2 = \rho_{L_1}(\omega^j + \omega^{-j})} (x^{2^{n-L+1}} + a_L x^{2^{n-L}} + \rho_{L_1})$$

Proof. It is clear that for $\omega \in \Omega(7)$, $\omega \notin \mathbb{F}_q$. But $\omega^{q+1} = 1$ implies that $\omega + \omega^{-1} \in \mathbb{F}_q$ and also by lemma 2.2 each irreducible factor must be quadratic. Hence

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

Now set $a_1 = \omega^j + \omega^{-j}$ for $j=1,2$ and 3. Then

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

For $2 \leq n \leq L_1$, lemma 2.2 implies that $Q_{2^n.7}(x)$ factors into $\varphi(2^n.7)/2$ distinct monic quadratic irreducible polynomials over $\mathbb{F}_q$. So, let $x^4 + a_1x^2 + 1 = (x^2 + u_1x + u_2)(x^2 + v_1x + v_2)$ where the co-efficients are in $\mathbb{F}_q$. Then by comparing the co-efficients and solving those equations we obtain $u_2 = v_2$ as $x^2 - a_1x + 1$ is irreducible over $\mathbb{F}_q$ which implies that $u_2 = v_2 = \pm\rho_1 \in \mathbb{F}_q$. Therefore $(x^4 + a_1x^2 + 1) = (x^2 + a_2x + \rho_2^2)(x^2 - a_2x + \rho_2^2)$ and $a_2^2 = \pm 2\rho_1 - a_1$. It is straightforward to show that $a_2 = \rho_2(\omega^{4j} + \omega^{-4j}) \in \mathbb{F}_q$ are the solutions of $a_2^2 = \pm 2\rho_1 - a_1$ where $\rho_2^2 = \rho_1$. Hence we can write

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

For $k=\text{even}$, $L_1=2$, $L=3$ and $q^2 \equiv 1 \pmod{2^L.7}$. So, let

$$(x^4 + a_2x^2 + \rho_2^2) = (x^2 + a_3x + \rho_2)(x^2 - a_3x + \rho_2)$$

Then $a_3^2 = 2\rho_2 - a_2$ and it is clear that $a_3, \rho_2 \in \mathbb{F}_q$. Therefore

$$Q_{2^3.7}(x) = \prod_{\rho_2 \in \Omega(2^2)} \prod_{a_2 = \rho_2(\omega^j + \omega^{-j})} \prod_{a_3^2 = 2\rho_2 - a_2} (x^2 + a_3x + \rho_2)$$

If $k=\text{odd}$, then $L_1 \geq 3$. For $3 \leq n \leq L_1$, we have $a_n = \rho_n(\omega^j + \omega^{-j}) \in \mathbb{F}_q$. Also $2\rho_{n-1} - a_n^2 = -a_{n-1}$. Then $(x^4 - a_{n-1}x^2 + \rho_{n-1}^2) = (x^2 + a_nx + \rho_{n-1})(x^2 -$

$a_n x + \rho_{n-1}$). Therefore

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

Similarly, for $n = L$, let $(x^4 - a_{L-1}x^2 + \rho_{L-1}^2) = (x^2 + a_L x + \rho_{L-1})(x^2 - a_L x + \rho_{L-1})$. Then we get $a_L, \rho_{L-1} \in \mathbb{F}_q$ satisfying $a_L^2 = 2\rho_{L-1} - a_{L-1}$. Hence

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

For $n > L$, the result follows from lemma 2.3 and $Q_{2^n,7}(x) = Q_{2^L,7}(x^{2^{n-L}})$. This completes the proof. $\square$

Now we consider the cases when $q \equiv 2, -3 \pmod{7}$ and $q \equiv 1 \pmod{4}$ i.e. $q \equiv 9 \pmod{28}$ and $q \equiv 25 \pmod{28}$. Then, we get $L_6 = L_1 + 1$ where $L_1 = 2 + v_2(7k + 2)$ or $L_1 = 2 + v_2(7k + 6)$ respectively. The following results are obtained for these cases.

Theorem 3.3. *Let $q \equiv 9 \pmod{28}$ or $q \equiv 25 \pmod{28}$ and $\omega \in \Omega(7)$, then we have the following factorization of $Q_{2^n,7}(x)$ over $\mathbb{F}_q$ as follows.*

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

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

$$Q_{2,7}(x) = \prod_{j=2k-1, k=1,2} (x^3 + (\omega^j + \omega^{2j} + \omega^{4j})x^2 + (\omega^{3j} + \omega^{5j} + \omega^{6j})x + 1)$$

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

$$Q_{2^n,7}(x) = \prod_{a_n, b_n, c_n} (x^3 + a_n x^2 + b_n x + c_n),$$

where a_n, b_n, c_n satisfies the following system of non-linear recurrence relations

$$\begin{aligned} 2b_n - a_n^2 &= a_{n-1} \\ -c_n^2 &= c_{n-1} \\ -2a_n c_n + b_n^2 &= b_{n-1} \end{aligned}$$

with initial values $(a_1, b_1, c_1) = ((\omega + \omega^2 + \omega^4), (\omega^3 + \omega^5 + \omega^6), 1)$ and $(a_1, b_1, c_1) = ((\omega^3 + \omega^5 + \omega^6), (\omega + \omega^2 + \omega^4), 1)$

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

$$Q_{2^n.7}(x) = \prod_{a_{L-1}, b_{L-1}, c_{L-1}} (x^{3 \cdot 2^{n-L+1}} + a_{L-1}x^{2^{n-L+2}} + b_{L-1}x^{2^{n-L+1}} + c_{L-1})$$

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 $0 \leq n \leq L-1$, $q^3 \equiv 1 \pmod{2^n \cdot 7}$. 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

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

Now suppose $2 \leq n \leq L-1$. As $Q_{2^n.7}(x) = Q_{2^{n-1}.7}(x^2)$, we assume $x^6 + a_{n-1}x^4 + b_{n-1}x^2 + c_{n-1} = (x^3 + ax^2 + bx + c)(x^3 + dx^2 + ex + f)$ which implies that $a = -d$, $c = -f$ and $b = e$. Hence we can write $x^6 + a_{n-1}x^4 + b_{n-1}x^2 + c_{n-1} = (x^3 + a_nx^2 + b_nx + c_n)(x^3 - a_nx^2 + b_nx - c_n)$. Using the above equation, we get a_n, b_n, c_n satisfies the following system of non-linear recurrence relations $2b_n - a_n^2 = a_{n-1}$, $-c_n^2 = c_{n-1}$ and $-2a_nc_n + b_n^2 = b_{n-1}$. We note that the above system has exactly two solutions for each n . The factorization for $Q_{2^L.7}(x)$ follows from lemma 2.1 and the result for $n > L$ follows from lemma 2.3 and $Q_{2^n.7}(x) = Q_{2^L.7}(x^{2^{n-L}})$. $\square$

Lastly, we consider the cases when $q \equiv -2, 3 \pmod{7}$ and $q \equiv 1 \pmod{4}$ i.e. $q \equiv 5 \pmod{28}$ and $q \equiv 17 \pmod{28}$. Then, we get $L_6 = L_1 + 1$ where $L_1 = 2 + v_2(7k + 1)$ or $L_1 = 2 + v_2(7k + 4)$ respectively. For these cases, we have the following results.

Theorem 3.4. Let $q \equiv 17 \pmod{28}$ or $q \equiv 5 \pmod{28}$. Then we have the following factorization of $Q_{2^n.7}(x)$ over $\mathbb{F}_q$ as given below.

(i) If $0 \leq n \leq L_1$, 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 $n \geq L = L_1 + 1$, then

$$Q_{2^n.7}(x) = \prod_{\rho_{L_1} \in \Omega(2^{L_1})} \prod_{a_L^2 = -7\rho_{L_1}} (x^{3 \cdot 2^{n-L+1}} + a_L x^{5 \cdot 2^{n-L}} - 3\rho_{L_1} x^{2^{n-L+2}} + \rho_{L_1} a_L x^{3 \cdot 2^{n-L}} + 3\rho_{L_1}^2 x^{2^{n-L+1}} + \rho_{L_1}^2 a_L x^{2^{n-L}} - \rho_{L_1}^3).$$

Proof. The factorization for $Q_7(x)$ and $Q_{2.7}(x)$ are obvious. For $2 \leq n \leq L-1$, each irreducible factor must have degree 6 and $\rho_n \in \Omega(2^n) \Rightarrow \rho_n \in F_q$. Also it is easy to verify that for $\rho_n^2 = \rho_{n-1}$,

$$\begin{aligned} & x^{12} + \rho_{n-1}x^{10} + \rho_{n-1}^2x^8 + \rho_{n-1}^3x^6 + \rho_{n-1}^4x^4 + \rho_{n-1}^5x^2 + \rho_{n-1}^6 \\ &= (x^6 + \rho_nx^5 + \rho_n^2x^4 + \rho_n^3x^3 + \rho_n^4x^2 + \rho_n^5x + \rho_n^6) \\ & \quad (x^6 - \rho_nx^5 + \rho_n^2x^4 - \rho_n^3x^3 + \rho_n^4x^2 - \rho_n^5x + \rho_n^6). \end{aligned}$$

Hence, for $0 \leq n \leq L-1$

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

Finally, suppose $n = L$. As $-7\rho_{L-1}$ is a square element in $\mathbb{F}_q$, let $a_L^2 = -7\rho_{L-1} \Rightarrow \pm a_L \in \mathbb{F}_q$. Then, one can easily verify that

$$\begin{aligned} & x^{12} + \rho_{L-1}x^{10} + \rho_{L-1}^2x^8 + \rho_{L-1}^3x^6 + \rho_{L-1}^4x^4 + \rho_{L-1}^5x^2 + \rho_{L-1}^6 \\ &= (x^6 + a_Lx^5 - 3\rho_{L-1}x^4 - \rho_{L-1}a_Lx^3 + 3\rho_{L-1}^2x^2 + \rho_{L-1}^2a_Lx - \rho_{L-1}^3) \\ & \quad (x^6 - a_Lx^5 - 3\rho_{L-1}x^4 + \rho_{L-1}a_Lx^3 + 3\rho_{L-1}^2x^2 - \rho_{L-1}^2a_Lx - \rho_{L-1}^3) \end{aligned}$$

in which all the factors are in $\mathbb{F}_q[x]$. Hence

$$\begin{aligned} Q_{2^n.7}(x) = & \prod_{\rho_{L-1} \in \Omega(2^{L-1})} \prod_{a_L^2 = -7\rho_{L-1}} (x^6 + a_Lx^5 - 3\rho_{L-1}x^4 - \rho_{L-1}a_Lx^3 \\ & + 3\rho_{L-1}^2x^2 + \rho_{L-1}^2a_Lx - \rho_{L-1}^3). \end{aligned}$$

The rest of the proof follows from lemma 2.3. $\square$

To illustrate and verify some of our results, we provide the following tables. The coefficient (a_n, b_n, c_n) for cubic and $(a_n, b_n, c_n, d_n, d_n, e_n)$ for factor having degree 6 of the irreducible factors of $Q_{2^n.7}(x)$ over $\mathbb{F}_q$ where $q = 37$ and 61 for Theorem 3.3 and 3.4 respectively are computed by using MATHEMATICA software and produce it in the form of a table as follows.

Example 1. Factorization of $Q_{2^n.7}(x)$ over $\mathbb{F}_q$, where $q = 37$.

n	1	2	3
(a_n, b_n, c_n)	(8,28,1)	(11,9,31)	(0,11,0,9,0,31)
for cubic and	(28,8,1)	(17,29,6)	(0,17,0,29,0,6)
$(a_n, b_n, c_n, d_n, d_n, e_n)$		(20,29,31)	(0,20,0,29,0,31)
for factor having		(26,9,6)	(0,26,0,9,0,6)
degree 6			

Example 2. Factorization of $Q_{2^n.7}(x)$ over $\mathbb{F}_q$, where $q = 61$.

n	1	2	3
$(a_n, b_n, c_n,$ $d_n, e_n)$	$(-1, 1, -1, 1,$ $-1, 1)$	$(11, -1, -11, 1,$ $11, -1)$ $(-11, -1, 11, 1,$ $-11, -1)$	$(4, 33, -17, -3, -4, -11)$ $(17, 28, -4, -3, -17, 11)$ $(-17, 28, 4, -3, 17, 11)$ $(-4, 33, 17, -3, 4, -11)$

4. Conclusion

In this paper, we observe many similar patterns of the factors obtained in [3]. The case for $q \equiv 3(\text{mod}4)$ will be dealt in a subsequent paper in order to give a complete and detailed study of the topic. The irreducible factors as discussed in [3] involve only monic polynomials of degree in power of 2. But in our case, we observe that the monic irreducible factors of $Q_{2^n.7}(x)$ have degree either a power of 2 or of the form 3.2^k and the number of terms for each irreducible factor does not exceed 7.

Acknowledgments

Authors are much thankful for financial assistance by CSIR under JRF scheme.

References

- [1] H. Meyn, Factorization of cyclotomic polynomials over finite fields, *Finite Fields Appl.*, **2** (1992), 439-442.
- [2] K. Motose, On the values of cyclotomic polynomials, *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*, **63** (2012), 87-104.
- [4] R. Lidl, H. Niederreiter, *Finite Fields*, Encyclopedia of Mathematics and its Application, Cambridge University Press, Cambridge (1997).
- [5] 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.