SOME SUBGROUPS OF $F_q^*$ AND EXPPLICIT FACTORS OF $x^{2^n} - 1 \in F_q[x]$

MANJIT SINGH

Communicated by Dianhua Wu

Abstract. Let $S_q$ denote the group of all square elements in the multiplicative group $F_q^*$ of a finite field $F_q$ of odd characteristic containing $q$ elements. Let $O_q$ be the set of all odd order elements of $F_q^*$. Then $O_q$ turns up as a subgroup of $S_q$. In this paper, we show that $O_q = \langle 4 \rangle$ if $q = 2t + 1$ and, $O_q = \langle t \rangle$ if $q = 4t + 1$, where $q$ and $t$ are odd primes. Further, we determine the coefficients of irreducible factors of $x^{2^n} - 1$ using generators of these special subgroups of $F_q^*$.

1. Introduction

Factoring polynomials over finite fields plays an important role in algebraic coding theory for the error-free transmission of information and cryptology for the secure transmission of information. Specifically, cyclic codes of length $m$ over finite fields are in one-to-one correspondence with the monic divisors of $x^m - 1$ over finite fields. Hereto, the availability of explicit factors of $x^m - 1$ over finite fields, especially irreducible polynomials over finite fields is useful for analyzing the structure and inner-relationship of codewords of a code and other areas of electrical engineering where linear feedback shift registers (LFSR) are used (see [1, 6, 8]).

Blake, Gao and Mullin [2] explicitly determined all the irreducible factors of $x^p - 1$ over $F_p$, where $p$ is a prime with $p \equiv 3 \pmod{4}$. Chen, Li and Tuerhong [4] gave the explicit factorization of $x^{2^m} - 1$ over $F_q$, where $p$ is an odd prime with $q \equiv 1 \pmod{p}$. In [3], Brochero Martínez, Giraldo Vergara and de Oliveira generalized the results in [4] by giving the explicit factorization of

Keywords: Polynomials over finite fields, Cyclotomic polynomials, Special groups.
Received: 25 December 2018, Accepted: 10 November 2019.

DOI: http://dx.doi.org/10.22108/toc.2019.114742.1612
Suppose that Lemma 2.2. results concerning subgroups and their generators of the multiplicative group \( F^* \) that the explicit factors of \( r \) computed the factors of \( r \) explicit factorization of \( 2 \). When \( q \) and \( r \) are distinct odd primes, Stein [12] computed the factors of \( \Phi_r(x) \) from the traces of the roots of \( \Phi_r(x) \) over prime field \( \mathbb{F}_q \). Assuming that the explicit factors of \( \Phi_r(x) \) are known, Tuxanidy and Wang [13] obtained the irreducible factors of \( \Phi_{2^r}(x) \) over \( \mathbb{F}_q \), where \( r > 1 \) is an arbitrary odd integer.

In this paper, we investigate the polynomial \( x^{2^n d} - 1 \) and study two subgroups of \( \mathbb{F}_q^* \). Further, we determine the coefficients of irreducible factors of \( x^{2^n t} - 1 \) over \( \mathbb{F}_q \) by using these two special subgroups of \( \mathbb{F}_q^* \), where \( q = 2t + 1 \) or \( q = 4t + 1 \) with odd primes \( q \) and \( t \). This paper also contributes an interesting result, that is, \( t \in \mathbb{F}_q^* \) such that the order of \( t \) is \( t \) for every odd primes \( q \) and \( t \) such that \( q = 4t + 1 \).

The paper is organized as follows: The necessary notation and some known results concerning the cyclotomic polynomials over finite fields are provided in Section 2. In Section 3, assuming \( d \) is an odd divisor of \( q - 1 \), the explicit factorization of \( x^{2^n d} - 1 \) over \( \mathbb{F}_q \) is reformulated in two different cases when \( q \equiv 1 \pmod{4} \) in Theorem 3.2 and, when \( q \equiv 3 \pmod{4} \) in Theorem 3.6. In Section 4, we record few results concerning subgroups and their generators of the multiplicative group \( \mathbb{F}_q^* \). Using these results, the coefficients of irreducible factors of \( x^{2^n t} - 1 \) over \( \mathbb{F}_q \) are obtained effortlessly when \( q \) and \( t \) are primes with \( q = 2t + 1 \) or \( q = 4t + 1 \). In order to illustrate our results, the explicit factorization of \( x^{2^n - 173} - 1 \in \mathbb{F}_{347}[x] \), \( x^{704} - 1 \in \mathbb{F}_{23}[x] \), \( x^{2^n - 37} - 1 \in \mathbb{F}_{149}[x] \) and \( x^{2^n - 13} - 1 \in \mathbb{F}_{53}[x] \) are obtained.

2. Cyclotomic factorization of \( x^{2^n d} - 1 \) over finite fields

For any integer \( n \geq 1 \), a well-known cyclotomic decomposition of \( x^n - 1 \) is as follows:

\[
x^n - 1 = \prod_{k \mid n} \Phi_k(x); \quad \Phi_k(x) = \prod_{\gcd(i,k)=1 \atop 0 \leq i \leq k} (x - \xi^i),
\]

where \( \Phi_k(x) \) is the \( k \)-th cyclotomic polynomial and \( \xi \) is a primitive \( k \)-th root of unity in some extension field of \( \mathbb{F}_q \). The degree of \( \Phi_k(x) \) is \( \phi(k) \), where \( \phi(k) \) is the Euler Totient function. Let \( e \) be the least positive integer such that \( q^e \equiv 1 \pmod{n} \). Then, in \( \mathbb{F}_q[x] \), \( \Phi_n(x) \) splits into the product of \( \phi(n)/e \) monic irreducible polynomials of degree \( e \). In particular, \( \Phi_n(x) \) is irreducible over \( \mathbb{F}_q \) if and only if \( e = \phi(n) \). Note that \( \Phi_n(x) \) is irreducible over \( \mathbb{F}_q \), then \( \Phi_m(x) \) is also irreducible over \( \mathbb{F}_q \) for every \( m \mid n \) (see [8, 10]).

**Lemma 2.1.** (see [14, Theorem 10.7] and [8, Theorem 3.75]) Let \( l \geq 2 \) be an integer and \( a \in \mathbb{F}_q^* \) such that the order of \( a \) is \( k \geq 2 \). Then the binomial \( x^l - a \in \mathbb{F}_q[x] \) is irreducible over \( \mathbb{F}_q \) if and only if the following conditions are satisfied:

(i) Every prime factor of \( l \) divides \( k \), but does not divide \( (q - 1)/k \);

(ii) If \( 4 \mid l \), then \( 4 \mid (q - 1) \).

**Lemma 2.2.** (see [14, Theorem 10.15]) Let \( f(x) \) be any irreducible polynomial over \( \mathbb{F}_q \) of degree \( l \geq 1 \). Suppose that \( f(0) \neq 0 \) and \( f(x) \) is of order \( e \) which is equal to the order of any root of \( f(x) \). Let \( k \)

DOI: http://dx.doi.org/10.22108/toc.2019.114742.1612
be a positive integer, then the polynomial $f(x^k)$ is irreducible over $\mathbb{F}_q$ if and only if the following three conditions are satisfied:

(i) Every prime divisor of $k$ divides $e$;
(ii) $\gcd(k, \frac{q^e-1}{e}) = 1$;
(iii) If $4|k$, then $4|(q^l-1)$.

**Lemma 2.3.** Suppose that $t$ is an odd prime such that $\gcd(2t, q) = 1$. Then in $\mathbb{F}_q[x]$ the following properties of cyclotomic polynomials hold:

(i) $\Phi_{2^kt}(x) = \Phi_{2^k}(x^t)$,
(ii) $\Phi_{2^k+n}(x) = \Phi_{2^k}(x^{2^n})$ for integers $k \geq 1$ and $r \geq 0$.
(iii) $\Phi_{2^n+e}(x) = \Phi_{2^k}(x^{2^{n-k}e})$ for all integer $n \geq k \geq 1$.

**Proof.** First and second part are given in [8, Exercise 2.57]. The third part is an immediate consequence of the parts (i) and (ii). \qed

Throughout in this paper, let $\mathbb{F}_q$ be a finite field of $q$ elements with $q = 2^st + 1$ for some integers $s \geq 1$ and $t$ is odd. Let $\alpha_{2^k}$ be a primitive $2^k$th root of unity of $\mathbb{F}_q^*$, where $0 \leq k \leq s$. The following result is immediate from the above description of decomposable cyclotomic polynomials.

**Lemma 2.4.** If $n$ is a positive integer and $d$ is an odd integer, then a factorization of $x^{2^nd} - 1$ into the product of decomposable cyclotomic polynomials over $\mathbb{F}_q$ is given by:

$$x^{2^nd} - 1 = \begin{cases} 
(x^d-1) \prod_{k=1}^{n} \Phi_{2^k}(x^d) & \text{for } 1 \leq n \leq s \\
(x^d-1) \prod_{k=1}^{s} \Phi_{2^k}(x) \prod_{r=1}^{n-s} \Phi_{2^{2^r}}(x^{2^rd}) & \text{for } n > s \geq 1,
\end{cases}$$

where $\Phi_{2^k}(x^d)$ for $1 \leq k \leq s$ and $\Phi_{2^r}(x^{2^rd})$ for $0 \leq r \leq n-s$ can be expressed as follows:

$$\Phi_{2^k}(x^d) = \prod_{1 \leq i \leq 2^{k-1}} (x^d - \alpha_{2^k}^{2i-1}) \text{ and } \Phi_{2^r}(x^{2^rd}) = \prod_{1 \leq i \leq 2^{r-1}} (x^{2^rd} - \alpha_{2^r}^{2i-1}).$$

3. **Factorization of $x^{2^nd} - 1$ over $\mathbb{F}_q$, when $q \equiv 1 \pmod{2d}$**

In this section, we reformulate the factorization of $x^{2^nd} - 1$ into irreducible factors over $\mathbb{F}_q$ recursively when $d$ is an odd divisor of $q - 1$. In order to determine the complete factorization of $x^{2^nd} - 1$ over $\mathbb{F}_q$, in view of Lemma 2.4, one needs to split the decomposable cyclotomic polynomials $\Phi_{2^k}(x^d)$ for $1 \leq k \leq s$ and $\Phi_{2^r}(x^{2^rd})$ for $1 \leq r \leq n-s$ into irreducible factors over $\mathbb{F}_q$.

**Lemma 3.1.** Let $d$ be an odd integer such that $q \equiv 1 \pmod{2^kd}$, where $1 \leq k \leq s$. Also, let $\gamma$ be a primitive $d$th root of unity in $\mathbb{F}_q^*$. Then, for any integer $r \geq 0$, the complete factorization of $\Phi_{2^k}(x^{2^rd})$
is given by:
\[ \Phi_{2k}(x^{2^r}) = \Phi_{2k}(x^{2^r}) \prod_{1 \leq i \leq 2^{k-1}} (x^{2^r} - \alpha_{2^k}^{2i-1} \gamma^j), \]

where
\[ \Phi_{2k}(x^{2^r}) = \begin{cases} 
\prod_{i=1}^{2^{k+r-1}} (x - \alpha_{2^k}^{2i-1}) & \text{if } k + r \leq s \\
\prod_{i=1}^{2^{k+r-s}} (x^{2^r} - \alpha_{2^k}^{2i-1}) & \text{if } k + r > s.
\end{cases} \]

Proof. For any integer \( r \geq 0 \) and \( 1 \leq k \leq s \), observe that
\[ \Phi_{2k}(x^{2^r}) = \prod_{1 \leq i \leq 2^{k-1}} (x^{2^r} - \alpha_{2^k}^{2i-1}) = \prod_{1 \leq i \leq 2^{k-1}} ((x^{2^r})^d - \alpha_{2^k}^{d(2i-1)}). \]

Let \( \gamma \) be a primitive \( d \)th root of unity in \( \mathbb{F}_{q^*} \). Then
\[ x^d - \alpha_{2^k}^{d(2i-1)} = \prod_{j=0}^{d-1} (x - \alpha_{2^k}^{2i-1} \gamma^j) \]

and hence
\[ \Phi_{2k}(x^{2^r}) = \prod_{1 \leq i \leq 2^{k-1}} (x^{2^r} - \alpha_{2^k}^{2i-1} \gamma^j) \]
\[ = \Phi_{2k}(x^{2^r}) \prod_{1 \leq i \leq 2^{k-1}} (x^{2^r} - \alpha_{2^k}^{2i-1} \gamma^j). \]

This completes the proof. \( \Box \)

**Theorem 3.2.** Let \( d \) be any odd integer and \( q \equiv 1 \pmod{2d} \). Then, for any integer \( n \geq 1 \), the factorization of \( x^{2^nd} - 1 \) over \( \mathbb{F}_q \) is given by:

\[ x^{2^nd} - 1 = \begin{cases} 
\prod_{j=0}^{d-1} (x - \gamma^j) \prod_{1 \leq i \leq n} (x - \alpha_{2^k}^{2i-1} \gamma^j) & \text{if } n \leq s \\
\prod_{j=0}^{d-1} (x - \gamma^j) \prod_{1 \leq i \leq n-s} (x - \alpha_{2^k}^{2i-1} \gamma^j) \prod_{1 \leq r \leq n-s} (x^{2^r} - \alpha_{2^k}^{2i-1} \gamma^j) & \text{if } n > s
\end{cases} \]

Further, if \( n > s \geq 2 \), the factorization \( x^{2^nd} - 1 \) over \( \mathbb{F}_q \) has \( 2^{n-1}(n-s+2)d \) irreducible factors, however if \( q \equiv 3 \pmod{4} \), all nonlinear factors in the factorization are reducible over \( \mathbb{F}_q \) except binomials \( x^2 + \gamma^j \) for all \( 0 \leq j \leq d-1 \).

DOI: http://dx.doi.org/10.22108/toc.2019.114742.1612
Proof. The desired factorization of $x^{2^n d} - 1$ over $\mathbb{F}_q$ follows immediately from Lemma 2.4 and Lemma 3.1. Further, when $n > s \geq 2$, the irreducibility of its nonlinear factors follows immediately from Lemma 2.1. For $q \equiv 3 \pmod{4}$, i.e. $s = 1$, the factorization of $x^{2^n d} - 1$ over $\mathbb{F}_q$ reduces to

$$x^{2^n d} - 1 = \prod_{j=0}^{d-1} \left( (x - \gamma^j)(x + \gamma^j) \prod_{1 \leq r \leq n-1} (x^{2^r} + \gamma^j) \right).$$

Again by Lemma 2.1, factors $x^{2^r} + \gamma^j$ are reducible over $\mathbb{F}_q$ for every $r \geq 2$ and $0 \leq j \leq d - 1$. \hfill \Box

To determine all irreducible factors of $x^{2^n d} - 1$ over $\mathbb{F}_q$ in the case $q \equiv 3 \pmod{4}$, we need to recall the following notation and results of [11].

Let $Q = q^2 = 2^u v + 1$, $u \geq 3$ and $2 \nmid v$. Let $\beta_{2^k}$ be a primitive $2^k$th root of unity in $\mathbb{F}_q^*$. Note that $\beta_{2^k} := \alpha_{2^k}$ when $\beta_{2^k} \in \mathbb{F}_q$.

(i) A quadratic character $\chi$ on $\langle \beta_{2^k} \rangle \subseteq \mathbb{F}_q^*$ is defined as

$$\chi(\beta_{2^k}) = \beta_{2^k}^{q+1} = \begin{cases} 1 & \text{if } 0 \leq k < u, \\ -1 & \text{if } k = u \end{cases}$$

(ii) A trace is a mapping $T : \mathbb{F}_Q \to \mathbb{F}_q$ defined as $T(x) = x + x^q$ for all $x \in \mathbb{F}_Q$. Further, for any integer $r \geq 1$, we define the $r$th trace $T_r : \mathbb{F}_Q \to \mathbb{F}_q$ such that $T_r(x) = T(x^r)$.

**Lemma 3.3.** [11, Lemma 2.6] For a fixed $k$, where $3 \leq k \leq u$, the cyclotomic polynomial $\Phi_{2^k}(x) = x^{2^{k-1}} + 1$ can be expressed into irreducible factors over $\mathbb{F}_q$ as follows:

$$\Phi_{2^k}(x) = \prod_{1 \leq i \leq 2^{k-3}} (x^2 \pm T(\beta_{2^k}^{2^{i-1}})x + \chi(\beta_{2^k})).$$

**Lemma 3.4.** [11, Theorem 3.3] If $q \equiv 3 \pmod{4}$ and $3 \leq k \leq u$. Then there are $2^{k-2}$ distinct traces $T(\beta_{2^k}^{2^{i-1}})$ such that the first $2^{k-3}$ traces are given by the following linear recursive sequence

$$T_{2^{i-1}}(\beta_{2^k}) = T(\beta_{2^k}) T(\beta_{2^{i-1}}) - \chi(\beta_{2^k}) T(\beta_{2^{i-3}})$$

and the rest of $2^{k-3}$ are $-T(\beta_{2^k}^{2^{i-1}})$. The initial terms of the sequence are $T(\beta_4) = 0$ and $T(\beta_{2^k}) = (T(\beta_{2^{k-1}}) + 2\chi(\beta_{2^k}))^{(t+1)/2}$ for $3 \leq k \leq u$.

**Theorem 3.5.** Assume that $q \equiv 3 \pmod{4}$ and $d$ is an odd integer with $q \equiv 1 \pmod{d}$. Then $\Phi_d(x^d) = \prod_{0 \leq j \leq d-1} (x^2 + \gamma^j)$ and for $3 \leq k \leq u$, the irreducible factorization of decomposable cyclotomic polynomial $\Phi_{2^k}(x^d)$ over $\mathbb{F}_q$ is given by:

$$\Phi_{2^k}(x^d) = \Phi_{2^k}(x) \prod_{1 \leq i \leq 2^{k-3}} (x^2 \pm T(\beta_{2^k}^{2^{i-1}})x + \chi(\beta_{2^k}) \gamma^{2^{2j}}).$$

Further, for any integer $r \geq 1$ and $3 \leq k \leq u$, the factorization of decomposable cyclotomic polynomial $\Phi_{2^k}(x^{2^r d})$ over $\mathbb{F}_q$ is given by:

$$\Phi_{2^k}(x^{2^r d}) = \Phi_{2^k}(x^{2^r}) \prod_{1 \leq i \leq 2^{k-3}} (x^{2^r + 1} \pm T(\beta_{2^k}^{2^{i-1}})x^{2^r} + \chi(\beta_{2^k}) \gamma^{2^{2j}}).$$

Furthermore, the decomposable polynomial $\Phi_{2^u}(x^{2^u d})$ is a product of $2^{u-2}$ irreducible trinomials over $\mathbb{F}_q$, while the decomposable polynomial $\Phi_{2^u}(x^{2^u d})$, where $2 \leq k \leq u-1$, is a product of $2^{k-2}$ reducible trinomials over $\mathbb{F}_q$.

**Proof.** Since $q$ is odd prime power, so $q^2 \equiv 1 \pmod{4}$, i.e., $Q \equiv 1 \pmod{4}$. Replacing $q$ by $Q$ and $\alpha_{2k}$ by $\beta_{2k}$ in the result of Lemma 3.1, we obtain the factorization of $\Phi_{2^k}(x^d)$ over $\mathbb{F}_Q$ such as

$$\Phi_{2^k}(x^d) = \Phi_{2^k}(x) \prod_{1 \leq j \leq d-1} (x - \beta_{2^k}^{2i-1} \gamma^j).$$

In particular, $\Phi_2(x^d) = x^d+1 = (x+1) \prod_{1 \leq j \leq d-1} (x + \gamma^j)$ and $\Phi_4(x^d) = x^{2d}+1 = (x^2+1) \prod_{1 \leq j \leq d-1} (x^2 + \gamma^j)$.

From Lemma 2.3(iii), for each $3 \leq k \leq u$, we express $\Phi_{2^k}(x^d)$ as follows:

$$\Phi_{2^k}(x^d) = \Phi_{2^{k-2}}(x^{4d}) = \prod_{0 \leq j \leq d-1} (x^4 - \beta_{2^{k-2}}^{2i-1} \gamma^j) = \prod_{0 \leq j \leq d-1} (x - \beta_{2^k}^{2i-1} \gamma^j)(x + \beta_{2^k}^{2i-1} \gamma^j)(x^2 + \beta_{2^k}^{2i-1} \gamma^j).$$

For any fixed $0 \leq j \leq d-1$, using the permutation $i \mapsto 2^{k-3} - i + 1$ on the set of integers $1 \leq i \leq 2^{k-3}$, we obtain

$$\prod_{i=1}^{2^{k-3}} (x^2 + \beta_{2^{k-1}}^{2i-1} \gamma^j) = \prod_{i=1}^{2^{k-3}} (x^2 - \beta_{2^{k-1}}^{-2i+1} \gamma^j).$$

Since $2^{k-1} | (q+1)$, so that $\beta_{2^{k-1}}^{(q+1)/2i-1} = 1$ and hence $\beta_{2^k}^{2(q-1)/2i-1} = \beta_{2^{k-1}}^{-2i+1}$. It follows that

$$\prod_{i=1}^{2^{k-3}} (x^2 - \beta_{2^{k-1}}^{2i-1} \gamma^j) = \prod_{i=1}^{2^{k-3}} (x^2 - \beta_{2^k}^{-q(2i-1)} \gamma^j).$$

Also, since $d$ is odd, the above expression can be written in the following form:

$$\prod_{0 \leq j \leq d-1} (x^2 - \beta_{2^{k-1}}^{2i-1} \gamma^j) = \prod_{0 \leq j \leq d-1} (x^2 - \beta_{2^k}^{-q(2i-1)} \gamma^j),$$

Thus, in view of the above discussion, a factorization of $\Phi_{2^k}(x^d)$ over $\mathbb{F}_Q$ is given by:

$$\Phi_{2^k}(x^d) = \prod_{1 \leq i \leq 2^{k-3}} \prod_{0 \leq j \leq d-1} (x - \beta_{2^{k-1}}^{2i-1} \gamma^j)(x + \beta_{2^{k-1}}^{q(2i-1)} \gamma^j)(x - \beta_{2^k}^{-q(2i-1)} \gamma^j)(x + \beta_{2^k}^{q(2i-1)} \gamma^j).$$

DOI: http://dx.doi.org/10.22108/toc.2019.114742.1612
The following observation is useful to shift the above factorization of $\Phi_{2k}(x^d)$ over the field $\mathbb{F}_q$. Note that $\beta_{2k}^{2i-1} \gamma^j$ and $-\beta_{2k}^{2i-1} \gamma^j$ are non-conjugate elements in $\mathbb{F}_q \setminus \mathbb{F}_q$ for any $1 \leq i \leq 2^k-3$. Therefore, the minimal polynomial of $\pm \beta_{2k}^{2i-1} \gamma^j$ is $x^2 \pm T(\beta_{2k}^{2i-1} \gamma^j)x + (\beta_{2k}^{2i-1} \gamma^j)^{q+1}$ in $\mathbb{F}_q[x]$. Note that $T(\beta_{2k}^{2i-1} \gamma^j) = \gamma^j T(\beta_{2k}^{2i-1})$ and $(\beta_{2k}^{2i-1} \gamma^j)^{q+1} = \gamma^{2j} \chi(\beta_{2k}^{2i-1}) \gamma(\beta_{2k})$. It follows that

$$\Phi_{2k}(x^d) = \prod_{1 \leq i \leq 2^k-3} \prod_{0 \leq j \leq d-1} (x^2 \pm \gamma^j T(\beta_{2k}^{2i-1})x + \gamma^{2j} \chi(\beta_{2k})).$$

For any integer $r \geq 1$, using the transformation $x \to x^{2^r}$, we have

$$\Phi_{2k}(x^{2^r d}) = \prod_{1 \leq i \leq 2^k-3} \prod_{0 \leq j \leq d-1} (x^{2^{r+1}} \pm \gamma^j T(\beta_{2k}^{2i-1})x^{2^r} + \chi(\beta_{2k}) \gamma^{2j})$$

$$= \Phi_{2k}(x^{2^r}) \prod_{1 \leq i \leq 2^k-3} \prod_{1 \leq j \leq d-1} (x^{2^{r+1}} \pm \gamma^j T(\beta_{2k}^{2i-1})x^{2^r} + \chi(\beta_{2k}) \gamma^{2j}).$$

By Lemma 2.2, every trinomial $x^{2^{r+1}} \pm \gamma^j T(\beta_{2k}^{2i-1})x^{2^r} + \chi(\beta_{2k}) \gamma^{2j}$ is reducible over $\mathbb{F}_q$ for $2 \leq k \leq u-1$ and irreducible over $\mathbb{F}_q$ for $k = u$. □

In the following theorem, we determine the factorization of $x^{2^u d} - 1$ over $\mathbb{F}_q$, when $q \equiv 3 \pmod{4}$ and $q \equiv 1 \pmod{d}$.

**Theorem 3.6.** If $q \equiv 3 \pmod{4}$ and $d | (q - 1)$, then $x^{2^u d} - 1$ can be expressed into a product of $d(2^{u-2}(n-u+2) + 1)$ irreducible factors over $\mathbb{F}_q$ as follows:

$$x^{2^u d} - 1 = (x^{2^u} - 1) \prod_{1 \leq j \leq d-1} (x \pm \gamma^j) \prod_{2 \leq k \leq u-1} \prod_{1 \leq j \leq 2^{k-2}} \prod_{1 \leq j \leq d-1} (x^{2^{r+1}} \pm \gamma^j T(\beta_{2k}^{2i-1})x^{2^r} - \gamma^{2j}),$$

Proof. By substituting $s = 1$ in Lemma 2.4, the factorization of $x^{2^u d} - 1$ over $\mathbb{F}_q$ can be reduced to

$$x^{2^u d} - 1 = (x^d - 1) \Phi_2(x^d) \prod_{1 \leq r \leq u-1} \Phi_{2^r}(x^d).$$

Now, we recall $u = \max\{r \in \mathbb{Z} : 2^r | (Q - 1)\}$ and reset the above factorization of $x^{2^u d} - 1$ as follows:

$$x^{2^u d} - 1 = (x^{2^u d} - 1) \prod_{k=2}^{u-1} \Phi_{2^k}(x^d) \prod_{r=u}^{n} \Phi_{2^r}(x^d)$$

$$= \prod_{j=0}^{d-1} ((x \pm \gamma^j)(x^{2^j} + \gamma^j) \prod_{k=3}^{u-1} \Phi_{2^k}(x^d) \prod_{r=0}^{n-u} \Phi_{2^r}(x^{2^r d})).$$

The result, therefore, follows from Theorem 3.5. □

DOI: http://dx.doi.org/10.22108/toc.2019.114742.1612
4. Main results

In this section, we introduce a direct method to obtain the coefficients of irreducible factors of \( \Phi_{2^{nt}}(x) \) and hence of \( x^{2^{nt}} - 1 \) over \( \mathbb{F}_q \) when \( q \) and \( t \) are odd primes such that either \( q = 2t + 1 \) or \( q = 4t + 1 \). First, we define \( S_q = \{ a^2 : a \in \mathbb{F}_q^* \} \) and \( O_q = \{ a \in \mathbb{F}_q^* : |a| \text{ is odd} \} \), where \(|a|\) denotes the order of \( a \in \mathbb{F}_q^* \). Note that \( S_3 = O_3 = \{ 1 \} \), \( O_5 = \{ 1 \} \subset \{ 1, 4 \} = S_5 \), \( S_7 = O_7 = \{ 1, 2, 4 \} \).

**Theorem 4.1.** For any odd prime power \( q \), \( S_q \) and \( O_q \) are subgroups of \( \mathbb{F}_q^* \) such that \( O_q \subseteq S_q \). Further, if \( q = 2^s t + 1 \) for some integer \( s \geq 1 \) and \( t \) is an odd integer, then \( O_q \) has \( t \) distinct elements and the set \( S_q \setminus O_q \) contains \( (2^{s-1} - 1)t \) elements of \( S_q \). Deduce, \( O_q = S_q \) if and only if \( q \equiv 3 \mod 4 \).

**Proof.** Let \( q = 2^s t + 1 \) with integer \( s \geq 1 \) and \( t \) is odd. Since \( S_q \) contains \((q-1)/2\) distinct elements of \( \mathbb{F}_q^* \), so the order of \( S_q \), i.e., \(|S_q| = 2^{s-1}t \). Now let \( a \in O_q \) with \(|a| = l \), then \( l \) is odd. By the converse of Lagrange’s theorem, \( l | (q - 1) \). Since \( l \) is odd, so \( l | t \) and hence \( a \in S_q \). It follows that \( O_q \subseteq S_q \) and \(|O_q| = \max \{ l : |a| = l \text{ and } a \in O_q \} = t \). Therefore, \( S_q \setminus O_q \) contains \((2^{s-1} - 1)t \) elements. Also, note that \( q \equiv 3 \mod 4 \), i.e., \( s = 1 \) if and only if \( S_q \setminus O_q = \emptyset \), i.e., all square elements are of odd order and hence \( O_q = S_q \). \( \square \)

**Theorem 4.2.** Let \( q \) and \( t \) be odd primes such that \( q = 2t + 1 \). Then \( S_q = O_q = \langle 4 \rangle \).

**Proof.** Since \( q = 2t + 1 \), where \( q \) and \( t \) are odd primes, so \( q \equiv 3 \mod 4 \). Thus, by Theorem 4.1, \( S_q = O_q \). Since \( q > 5 \), so \( 4 \in \mathbb{F}_q^* \). Clearly, \( 4 \in O_q \). Since \( O_q \) is cyclic group of prime order \( t \), so any element of \( O_q \), except 1, works as a generator and hence \( O_q = \langle 4 \rangle \). \( \square \)

**Lemma 4.3.** [7, Corollary 7.10] If \( p \) is an odd prime, then
\[
\left( \frac{2}{p} \right) = (-1)^{(p^2 - 1)/8}.
\]

**Theorem 4.4.** Let \( q \) and \( t \) be odd primes such that \( q = 4t + 1 \). Then \( t, \sqrt{t} \in S_q \). Further, the following holds:

(i) \( O_q = \langle t \rangle \).

(ii) \( S_q = \langle 4 \rangle \) and \( O_q = \langle 16 \rangle \) for \( q > 13 \).

**Proof.** Let \( q = 4t + 1 \), where \( q \) and \( t \) are primes. Since \( 4, -1 \in S_q \) and \( 4t = -1 \in \mathbb{F}_q^* \), so that \( t \in S_q \) and hence \( \sqrt{t} \in \mathbb{F}_q^* \). From Lemma 4.3, it follows that \( 2 \notin S_q \) as \( q \equiv 5 \mod 8 \). Since \( 2\sqrt{t} = \sqrt{-1} \) or \( 2\sqrt{t} = -\sqrt{-1} \) with 2 and \( \pm \sqrt{-1} \) do not belong to \( S_q \), so that \( \sqrt{t} \in S_q \) because the product of a square and non-square element always a non-square element in \( \mathbb{F}_q^* \).

(i) In this item, we shall show that \( t \) is an element of \( O_q \) of the order \( t \), that is \(|t| = t\), where \(|t|\) denotes the order of \( t \) in \( \mathbb{F}_q^* \). Since \( t \in S_q \), so \(|t| = t \) or \( 2t \). On contrary, we assume \(|t| = 2t \). This yields that \( t^t \equiv -1 \mod q \). Using the fact \( 4t \equiv -1 \mod q \) and applying the arithmetic in \( \mathbb{F}_q \), we have \( t^{(t-1)/2} \equiv 2 \equiv 0 \mod q \). This implies \( 2 \in S_q \) or \(-2 \in S_q \), a contradiction.
Further, for primitive $T$. Example 4.2. follows that and $T$. Example 4.1.

Proof. Theorem 4.8.

Corollary 4.5. Let $q$ and $t$ be odd primes such that $q = 4t + 1$. Then $t \in \mathbb{F}_q^*$ such that the order of $t$ is $t$.

Remark 4.6. Since $t \in \mathcal{O}_q = \langle 16 \rangle$, so $t = 16^i$ for some unique integer $1 \leq i \leq t - 1$. Thus $\sqrt{t} = 4^i$ and hence $\sqrt{t} \in \mathcal{S}_q$. For example taking $q = 53$, then $t = 13 = 16^6$ and $\sqrt{t} = 16^3 = 15 \in \mathcal{O}_{53}$.

In the following two theorems, we obtain the factorization of $x^{2n^t} - 1$ into irreducible factors over $\mathbb{F}_q$ when either $q = 2t + 1$ or $q = 4t + 1$.

Theorem 4.7. Let $q$ and $t$ be odd primes such that $q = 2t + 1$, then

$$x^{2nt} - 1 = \prod_{0 \leq j \leq t-1} (x + 4^j) \prod_{2 \leq k \leq u-1 \atop 1 \leq j \leq 2k-2} (x^2 - 4^j T(\beta_{2k}^{2j-1}) x + 4^{2j}) \prod_{0 \leq r \leq n-u \atop 1 \leq j \leq 2r-3} (x^{2r+1} + 4^j T(\beta_{2r}^{2j-1}) x^{2r} - 4^{2j}).$$

Proof. The proof follows immediately by using Theorem 3.4, Theorem 3.6 and Theorem 4.2.

Theorem 4.8. Let $q$ and $t$ be odd primes such that $q = 4t + 1$. Then the factorization of $x^{2nt} - 1$ into the product of $2nt$ irreducible polynomials over $\mathbb{F}_q$ is given by:

$$x^{2nt} - 1 = \prod_{j=0}^{t-1} \left((x + 16^j)(x + \sqrt{-1} \cdot 16^j) \prod_{1 \leq r \leq n-2} (x^{2r} \pm \sqrt{-1} \cdot 16^j)\right).$$

Proof. The proof follows immediately from Theorem 3.2 and Theorem 4.4.

Example 4.1. Let $q = 347 = 2 \cdot 173 + 1$. Then $s = 1$, $t = 173$ and $u = 3$. Now $\beta_2 = -1$, $T(\beta_4) = 0$ and $T(\beta_8) = \sqrt{-2} = (-2)^{87} = 107$. By Theorem 4.2, 4 is a primitive 173th root of unity in $\mathbb{F}_{347}^*$. It follows that $x^{173} - 1 = \prod_{j=0}^{172} (x - 4^j)$ and $x^{173} + 1 = \prod_{j=0}^{172} (x + 4^j)$. Also $x^{346} + 1 = \prod_{j=0}^{172} (x^2 + 4^j)$. Further, for $n \geq 3$, by Theorem 4.7, the factorization of $x^{2n^{173}} - 1$ into 173($2n-1$) irreducible factors over $\mathbb{F}_{347}$ is given by:

$$x^{2n^{173}} - 1 = \prod_{0 \leq j \leq 172} (x + 4^j) (x^2 + 4^{2j}) \prod_{0 \leq r \leq n-3} (x^{2r+1} + 4^j \cdot 107 x^{2r} - 4^{2j}).$$

Example 4.2. Let $q = 23 = 2 \cdot 11 + 1$. Then $s = 1$, $t = 11$ and $u = 4$. In $\mathbb{F}_{23}$, $\beta_2 = -1$, $T(\beta_4) = 0$, $T(\beta_8) = \sqrt{2} = 2^6 = -5$ and $T(\beta_{16}) = \sqrt{-5 - 2} = (-7)^6 = 4$, $T_3(\beta_{16}) = 7$. By Theorem 4.2, 4 is a primitive 11th root of unity in $\mathbb{F}_{11}^*$. It follows that $x^{11} - 1 = \prod_{j=0}^{10} (x - 4^j)$ and $x^{11} + 1 = \prod_{j=0}^{10} (x + 4^j)$.
Also $x^{22} + 1 = \prod_{j=0}^{10} (x^2 + 4^j)$. Further, by Theorem 4.7, the factorization of $x^{352} - 1$ into 143 irreducible factors over $\mathbb{F}_{23}$ is given as:

$$x^{352} - 1 = \prod_{0 \leq j \leq 10} \left( (x + 4^j) \prod_{1 \leq i \leq 2^{k-2}} (x^2 - 4^j \mathbb{T}(\beta_{2^i-1}^{2^k-1})x + 4^{2j}) \right) \prod_{1 \leq i \leq 2} (x^2 + 4^i \mathbb{T}(\beta_{2^i-1}^{2} - 1)x - 4^{2j})(x^4 + 4^i \mathbb{T}(\beta_{16}^{2(2i-1)})x^2 - 4^{2j})$$

$$= (x^{44} - 1) \prod_{0 \leq j \leq 10, \eta \in \{4, 7\}} \left( (x^2 + 4^j \cdot 5x + 4^{2j}) \right) \cdot (x^2 + 4^j \eta x - 4^{2j})(x^4 + 4^j \eta x^2 - 4^{2j})$$.  

Furthermore, using recursive approach, the factorization of $x^{704} - 1$ into 187 irreducible factors over $\mathbb{F}_{23}$ is given by

$$x^{704} - 1 = (x^{352} - 1) \prod_{0 \leq j \leq 10, \eta \in \{4, 7\}} (x^8 + 4^j \eta x^4 - 4^{2j})$$.

**Example 4.3.** Let $q = 149 = 4 \cdot 37 + 1$. Then $s = 2$, $t = 37$. By Theorem 4.4, $\alpha_4 = \sqrt{-1} = \sqrt{148} = 2\sqrt{37} = 2 \cdot 16^9 = -44$. Using Theorem 4.8, the factorization of $x^{2^n \cdot 37} - 1$ over $\mathbb{F}_{149}$ can be written into a product of $74n$ irreducible factors as follows:

$$x^{2^n \cdot 37} - 1 = \prod_{j=0}^{36} \left( (x + 16^j)(x + 44 \cdot 16^j) \prod_{1 \leq r \leq n-2} (x^{2r} + 44 \cdot 16^j) \right)$$.  

**Example 4.4.** Let $q = 53 = 4 \cdot 13 + 1$. Then $s = 2$, $t = 13$. By Theorem 4.4, $\alpha_4 = \sqrt{-1} = \sqrt{52} = 2\sqrt{13} = 2 \cdot 16^3 = 30$. Using Theorem 4.8, the factorization of $x^{2^n \cdot 13} - 1$ over $\mathbb{F}_{53}$ can be written into a product of $26n$ irreducible factors as follows:

$$x^{2^n \cdot 13} - 1 = \prod_{j=0}^{12} \left( (x + 16^j)(x + 30 \cdot 16^j) \prod_{1 \leq r \leq n-2} (x^{2r} + 30 \cdot 16^j) \right)$$.  

**Acknowledgments**

The author would like to sincerely thank the anonymous referees for a careful reading and helpful comments. Their suggestions were valuable to create an improved final version.

**References**


**Manjit Singh**

Department of Mathematics, Deenbandhu Chhotu Ram University of Science and Technology
Murthal-131039, Sonepat, India

Email: manjitsingh.math@gmail.com

DOI: http://dx.doi.org/10.22108/toc.2019.114742.1612