Hindawi
Journal of Mathematics
Volume 2021, Article ID 6626422, 10 pages
https://doi.org/10.1155/2021/6626422

Research Article

Revisiting the Factorization of $x^n + 1$ over Finite Fields with Applications

Arunwan Boripan [1] **and Somphong Jitman** [2]

[1]Department of Mathematics, Faculty of Science, Ramkhamhaeng University, Bangkok 10240, Thailand
[2]Department of Mathematics, Faculty of Science, Silpakorn University, Nakhon Pathom 73000, Thailand

Correspondence should be addressed to Somphong Jitman; sjitman@gmail.com

Received 29 November 2020; Accepted 12 December 2020; Published 7 January 2021

Academic Editor: Marco Fontana; fontana@mat.uniroma3.it

The polynomial $x^n + 1$ over finite fields has been of interest due to its applications in the study of negacyclic codes over finite fields. In this paper, a rigorous treatment of the factorization of $x^n + 1$ over finite fields is given as well as its applications. Explicit and recursive methods for factorizing $x^n + 1$ over finite fields are provided together with the enumeration formula. As applications, some families of negacyclic codes are revisited with more clear and simpler forms.

1. Introduction

In coding theory, the polynomial $x^n + 1$ over finite fields plays an important role in the study of negacyclic codes (see [1–5] and references therein). Precisely, a negacyclic code of length n over $\mathbb{F}_q$ can be uniquely determined by an ideal in the principal ring $\mathbb{F}_q[x]/\langle x^n + 1\rangle$ generated by a monic divisor of $x^n + 1$. A brief discussion on the factorization of $x^n + 1$ over finite fields $\mathbb{F}_q$ has been given in [3, 4]. In the case where the characteristic of $\mathbb{F}_q$ is even, the factorization of $x^n + 1 = x^n - 1$ over $\mathbb{F}_q$ has been given and applied in the study of cyclic codes over finite fields in [6]. In [7, 8], an explicit form of the factorization of $x^{2^i} + 1$ over finite fields of odd characteristic has been established. Some results on the factorization of $x^n - \lambda$ over finite fields have been presented in [5].

In this paper, we focus on the factorization of $x^n + 1$ over finite fields $\mathbb{F}_q$ for arbitrary positive integers n and all odd prime powers q. If the characteristic of $\mathbb{F}_q$ is p, we have $x^{p^s n} + 1 = (x^n + 1)^{p^s}$, for all integers $n \geq 1$ and $s \geq 0$. It is therefore sufficient to study the factorization of $x^n + 1$ over $\mathbb{F}_q$ such that n is coprime to q. Here, we write $n = 2^i n'$ for some integer $i \geq 0$ and odd positive integer n' such that $\gcd(n', q) = 1$.

Before proceeding to the general results, we consider a pattern on the factorization of $x^{2^i 11} + 1$ over $\mathbb{F}_5$. We have

$$\begin{aligned}
x^{2\cdot 11} + 1 &= f_1(x) f_2(x) f_3(x) f_4(x) f_5(x) f_6(x),\\
x^{2^2\cdot 11} + 1 &= f_1\left(x^2\right) f_2\left(x^2\right) f_3\left(x^2\right) f_4\left(x^2\right) f_5\left(x^2\right) f_6\left(x^2\right),\\
&\vdots\\
x^{2^i\cdot 11} + 1 &= f_1\left(x^{2^{i-1}}\right) f_2\left(x^{2^{i-1}}\right) f_3\left(x^{2^{i-1}}\right) f_4\left(x^{2^{i-1}}\right)\\
&\quad \cdot f_5\left(x^{2^{i-1}}\right) f_6\left(x^{2^{i-1}}\right),
\end{aligned} \tag{1}$$

for all $i \geq 1$, where $f_1(x) = x + 2$, $f_2(x) = x + 3$, $f_3(x) = x^5 + x^4 + x^3 + 2x^2 + x + 2$, $f_4(x) = x^5 + 2x^4 + x^3 + 2x^2 + 3x + 2$, $f_5(x) = x^5 + 3x^4 + x^3 + 3x^2 + 3x + 3$, and $f_6(x) = x^5 + 4x^4 + x^3 + 3x^2 + x + 3$. It is easily seen that the factorization can be determined recursively on the exponent i of 2 and the number of monic irreducible factors of $x^{2^i 11} + 1$ is a constant independent of $i \geq 2$.

In this paper, a complete study on the above pattern of the factorization of $x^{2^i n'} + 1$ over $\mathbb{F}_q$ is given. Precisely, we prove that there exists a positive integer k such that the number of monic irreducible factors of $x^{2^i n'} + 1$ over $\mathbb{F}_q$

becomes a constant for all positive integers $i \geq k$. In the cases where $\mathrm{ord}_{n'}(q)$ is odd, a complete recursive factorization of $x^{2^i n'} + 1$ over $\mathbb{F}_q$ is provided together with a recursive formula for the number of its monic irreducible factors for all positive integers i. In the cases where $\mathrm{ord}_{n'}(q)$ is even, a recursive factorization of $x^{2^i n'} + 1$ over $\mathbb{F}_q$ is given for all positive integers $i \geq k$. As applications, constructions and enumerations of some negacyclic codes of lengths $2^i n'$ over $\mathbb{F}_q$ are given based on the above results.

The paper is organized as follows. Preliminary concepts and results on the factorization of $x^n + 1$ over finite fields are recalled in Section 2. In Section 3, the number theoretical results and properties of q-cyclotomic cosets required in the study of the factorization of $x^{2^i n'} + 1$ are established. Recursive methods for factorizing $x^{2^i n'} + 1$ and enumerating its monic irreducible factors are given in Section 4. Applications in the study of negacyclic codes over finite fields are revisited in Section 5.

2. Preliminary

In this section, basic concepts and tools used in the study of the factorization of $x^n + 1$ over finite fields and the enumeration of its monic irreducible factors are recalled.

For a positive integer a and an integer s, the notation $2^s \| a$ is used whenever s is the largest integer such that a is divisible by 2^s, or equivalently, $2^s | a$ but $2^{s+1} \nmid a$. For an integer a and a positive integer n, denote by $\Theta_n(a)$ the additive order of a modulo n. In the case where $\gcd(a, n) = 1$, denote by $\mathrm{ord}_n(a)$ the multiplicative order of a modulo n. By abuse of notation, we write $\mathrm{ord}_1(a) = 1$.

For a prime power q, a positive integer n coprime to q, and an integer $0 \leq a < n$, the *q-cyclotomic coset modulo n containing a* is defined to be

$$Cl_{q,n}(a) = \left\{ aq^j \, (\mathrm{mod}\, n) | j = 0, 1, 2, \ldots \right\}. \tag{2}$$

It is not difficult to see that $Cl_{q,n}(a) = \{aq^j \,(\mathrm{mod}\, n) | 0 \leq j < \mathrm{ord}_{\Theta_n(a)}(q)\}$ and $|Cl_{q,n}(a)| = \mathrm{ord}_{\Theta_n(a)}(q)$. Moreover, $\Theta_n(a) = \Theta_n(j)$ for all $j \in Cl_{q,n}(a)$. Let $S_q(n)$ denote a complete set of representatives of the q-cyclotomic cosets modulo n, and let α be a primitive nth root of unity in some extension field of $\mathbb{F}_q$. It is well known (see [9]) that

$$x^n - 1 = \prod_{a \in S_q(n)} f_a(x), \tag{3}$$

where

$$f_a(x) = \prod_{j \in Cl_{q,n}(a)} \left(x - \alpha^j \right), \tag{4}$$

is the minimal polynomial of α^a over $\mathbb{F}_q$ referred as the irreducible polynomial induced by $Cl_{q,n}(a)$.

In [10], a basic idea for the factorization of $x^{2^i n'} + 1$ is given using (3) and the following lemmas.

Lemma 1 (see [10], Lemma 2). *Let q be an odd prime power, and let n' be an odd positive integer such that $\gcd(q, n') = 1$. Let $i \geq 0$ and $0 \leq a < 2^{i+1} n'$ be integers. Then, the elements in $Cl_{q,2^{i+1}n'}(a)$ have the same parity.*

Lemma 2 (see [10], Lemma 3). *Let q be an odd prime power, and let n' be an odd positive integer such that $\gcd(q, n') = 1$. Let $i \geq 0$ and $0 \leq a < 2^{i+1} n'$ be integers. Then, the polynomial $f_a(x)$ induced by $Cl_{q,2^{i+1}n'}(a)$ is a divisor of $x^{2^i n'} + 1$ if and only if a is odd.*

From Lemma 1, the parity of a representative of $Cl_{q,2^{i+1}n'}(a)$ is independent of its choices. By Lemma 2, the monic irreducible divisors of $x^{2^i n'} + 1$ are induced by the q-cyclotomic cosets modulo $2^{i+1} n'$ containing odd integers. Let $\mathrm{SO}_q(n)$ (resp., $\mathrm{SE}_q(n)$) denote a complete set of representatives of the q-cyclotomic cosets containing odd integers (resp., even integers) modulo n. It follows that

$$x^{2^i n'} + 1 = \frac{x^{2^{i+1} n'} - 1}{x^{2^i n'} - 1} = \prod_{a \in SO_q(2^{i+1} n')} f_a(x), \tag{5}$$

for all $i \geq 0$.

For a positive integer n and a prime power q, let $N_q(n)$ denote the number of monic irreducible factors of $x^n + 1$ over $\mathbb{F}_q$. Based on ([3], equation 3.1), it can be deduced that

$$N_q\left(2^i n'\right) = \sum_{d | n'} \frac{\phi\left(2^{i+1} d\right)}{\mathrm{ord}_{2^{i+1} d}(q)}. \tag{6}$$

As discussed above, the q-cyclotomic cosets modulo $2^{i+1} n'$ containing odd integers are key to determine the factorization of $x^{2^i n'} + 1$ over $\mathbb{F}_q$ and the enumeration of its monic irreducible factors. Properties of these cosets are studied in Section 3.

3. Number Theoretical Results and Cyclotomic Cosets

In this section, number theoretical results required in the factorization of $x^{2^i n'} + 1$ are derived. Subsequently, properties of q-cyclotomic cosets modulo $2^{i+1} n'$ containing odd integers are established for all positive integers i and odd positive integers n'. These results are key in the study of the factorization of $x^{2^i n'} + 1$ in Section 4.

A relation on the carnality of the q-cyclotomic costs containing odd integers a and $a + 2^i n'$ modulo $2^{i+1} n'$ is given in the following lemma.

Lemma 3. *Let q be an odd prime power, and let n' be an odd positive integer such that $\gcd(q, n') = 1$. Then, $|Cl_{q,2^{i+1}n'}(a)| = |Cl_{q,2^{i+1}n'}(a + 2^i n')|$ for all odd integers a and for all positive integers i.*

Proof. Let a be an odd integer, and let i be a positive integer. Then,

$$\Theta_{2^{i+1}n'}(a) = \frac{2^{i+1}n'}{\gcd\left(2^{i+1}n', a\right)} = \frac{2^{i+1}n'}{\gcd\left(n', a\right)} = \frac{2^{i+1}n'}{\gcd\left(n', a+2^i n'\right)},$$
$$= \frac{2^{i+1}n'}{\gcd\left(2^{i+1}n', a+2^i n'\right)} = \Theta_{2^{i+1}n'}\left(a+2^i n'\right). \tag{7}$$

Hence,

$$\left|Cl_{q,2^{i+1}n'}(a)\right| = \mathrm{ord}_{\Theta_{2^{i+1}n'}(a)}(q) = \mathrm{ord}_{\Theta_{2^{i+1}n'}\left(a+2^i n'\right)}(q)$$
$$= \left|Cl_{q,2^{i+1}n'}\left(a+2^i n'\right)\right|, \tag{8}$$

as desired. □

Properties of q-cyclotomic cosets with $q \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$ are given separately in the following sections.

3.1. $q \equiv 3$ (mod 4). In this section, we focus on properties of q-cyclotomic cosets in the case where $q \equiv 3 \pmod 4$.

First, an explicit formula for $\mathrm{ord}_{2^i}(q)$ is recalled for all odd prime powers $q \equiv 3 \pmod 4$ and positive integers i. This result can be derived from ([11], Proposition 1). For completeness, a detailed proof is given.

Lemma 4. *Let q be an odd prime power, and let β be the positive integer such that $2^\beta \| (q^2-1)$. Let i be a positive integer. If $q \equiv 3 \pmod 4$, then*

$$\mathrm{ord}_{2^i}(q) = \begin{cases} 1, & \text{if } i = 1, \\ 2, & \text{if } 2 \le i \le \beta, \\ 2^{i-\beta+1}, & \text{if } i \ge \beta+1. \end{cases} \tag{9}$$

Proof. Assume that $q \equiv 3 \pmod 4$. Then, $2 \| (q-1)$ and $2^i | (q^2-1)$, for all $2 \le i \le \beta$. Since $q^3 - 1 = (q-1)(q^2+q+1)$ and q^2+q+1 is odd, we have $2 \| (q^3-1)$. Hence, $\mathrm{ord}_2(q) = 1$ and $\mathrm{ord}_{2^i}(q) = 2$, for all $2 \le i \le \beta$.

Assume that $i \ge \beta+1$. Since $q \equiv 3 \pmod 4$, it follows that $q^{2^j} \equiv 1 \pmod 4$, for all $j \ge 1$. Hence, $2 \| (q^{2^j}+1)$, for all $j \ge 1$. Since $(q^{2^{i-\beta}}-1)(q^{2^{i-\beta}}+1) = q^{2^{i-\beta+1}}-1 = (q^2-1)\prod_{j=1}^{i-\beta}(q^{2^j}+1)$, we have $2^i \| (q^{2^{\beta-i+1}}-1)$ and $2^i \nmid (q^{2^t}-1)$, for all $t \le \beta+i$. Hence, $\mathrm{ord}_{2^i}(q) = 2^{i-\beta+1}$, for all $i \ge \beta+1$. □

Properties of q-cyclotomic cosets modulo $2^{i+1}n'$ containing odd integers are established in Proposition 1.

Proposition 1. *Let q be a prime power such that $q \equiv 3 \pmod 4$, and let n' be an odd positive integer such that $\gcd(q, n') = 1$. Let $\lambda \ge 0$ be the integer such that $2^\lambda \| \mathrm{ord}_{n'}(q)$, and let β be the positive integer such that $2^\beta \| (q^2-1)$. Then, the following statements hold:*

(i) If $\lambda = 0$, then the following statements hold:

(a) $Cl_{q,2^{i+1}n'}(a) \ne Cl_{q,2^{i+1}n'}(a+2^i n')$ all odd integers a and integers $2 \le i \le \beta-1$

(b) $Cl_{q,2^{i+1}n'}(a) = Cl_{q,2^{i+1}n'}(a+2^i n') = Cl_{q,2^i n'}(a) \cup (Cl_{q,2^i n'}(a)+2^i n')$ for all odd integers a and integers $i = 1$ or $i \ge \beta$

(ii) If $\lambda > 0$, then the following statements hold:

(a) $Cl_{q,2^{\lambda+\beta-1}n'}(1) \ne Cl_{q,2^{\lambda+\beta-1}n'}(1+2^{\lambda+\beta-2}n')$

(b) $Cl_{q,2^{i+1}n'}(a) = Cl_{q,2^i n'}(a) \cup (Cl_{q,2^i n'}(a)+2^i n')$ for all odd integers a and integers $i \ge \lambda+\beta-1$

Proof. First, we observe that $\beta \ge 3$, $2 \| (q-1)$ and $2^{\beta-1} \| (q+1)$.

To prove (i), assume that $\lambda = 0$. In this case, $\mathrm{ord}_{n'}(q)$ is odd which implies that $\mathrm{ord}_{\Theta_{n'}(a)}(q)$ is odd for all odd positive integers a.

To prove (a), let a be an odd integer, and let i be an integer such that $2 \le i \le \beta-1$. By Lemma 4, it follows that $\mathrm{ord}_{2^i}(q) = 2 = \mathrm{ord}_{2^{i+1}}(q)$. Since $\mathrm{ord}_{\Theta_{n'}(a)}(q)$ is odd, it can be deduced that $\mathrm{ord}_{\Theta_{2^{i+1}n'}(a)}(q) = \mathrm{ord}_{2^{i+1}\Theta_{n'}(a)}(q) = lcm(\mathrm{ord}_{2^{i+1}}(q), \mathrm{ord}_{\Theta_{n'}(a)}(q)) = lcm(\mathrm{ord}_{2^i}(q), \mathrm{ord}_{\Theta_{n'}(a)}(q)) = \mathrm{ord}_{\Theta_{2^i n'}(a)}(q)$. Suppose that $Cl_{q,2^{i+1}n'}(a) = Cl_{q,2^{i+1}n'}(a+2^i n')$. Since $a \not\equiv a+2^i n' \pmod{2^{i+1}n'}$, there exists $0 < j < \mathrm{ord}_{\Theta_{2^{i+1}n'}(a)}(q)$ such that $a+2^i n' \equiv aq^j \pmod{2^{i+1}n'}$. Hence, we have $a \equiv aq^j \pmod{2^i n'}$ which implies that $\mathrm{ord}_{\Theta_{2^i n'}(a)}(q) \le j < \mathrm{ord}_{\Theta_{2^{i+1}n'}(a)}(q) = \mathrm{ord}_{\Theta_{2^i n'}(a)}(q)$, a contradiction. Therefore, $Cl_{q,2^{i+1}n'}(a) \ne Cl_{q,2^{i+1}n'}(a+2^i n')$, as desired.

To prove (b), let a be an odd integer, and let i be an integer such that $i = 1$ or $i \ge \beta$. By Lemma 4, we have $\mathrm{ord}_{2^{i+1}}(q) = 2\,\mathrm{ord}_{2^i}(q)$. Since $\mathrm{ord}_{n'}(q)$ is odd, we have $\mathrm{ord}_{2^{i+1}n'}(q) = lcm(\mathrm{ord}_{2^{i+1}}(q), \mathrm{ord}_{n'}(q)) = lcm(2\,\mathrm{ord}_{2^i}(q), \mathrm{ord}_{n'}(q)) = 2\,\mathrm{ord}_{2^i n'}(q)$ which implies that $aq^{\mathrm{ord}_{2^i n'}(q)} \not\equiv a \pmod{2^{i+1}n'}$. Since $aq^{\mathrm{ord}_{2^i n'}(q)} \equiv a \pmod{2^i n'}$, we have $aq^{\mathrm{ord}_{2^i n'}(q)} \equiv a+2^i n' \pmod{2^{i+1}n'}$. Hence, $a+2^i n' \in Cl_{q,2^{i+1}n'}(a)$ which implies that $Cl_{q,2^{i+1}n'}(a) = Cl_{q,2^{i+1}n'}(a+2^i n')$. This proves the first equality.

For the second equality, let $b \in Cl_{q,2^{i+1}n'}(a)$. Then, $b \equiv aq^j \pmod{2^{i+1}n'}$ for some $0 \le j < \mathrm{ord}_{\Theta_{2^{i+1}n'}(a)}(q)$. It follows that $b \equiv aq^j \pmod{2^i n'}$. If $b < 2^i n'$, then $b \in Cl_{q,2^i n'}(a)$. Otherwise, $b - 2^i n' \in Cl_{q,2^i n'}(a)$ which implies that $b \in Cl_{q,2^i n'}(a) + 2^i n'$. Hence, $Cl_{q,2^{i+1}n'}(a) \subseteq Cl_{q,2^i n'}(a) \cup (Cl_{q,2^i n'}(a) + 2^i n')$. Since $Cl_{q,2^i n'}(a)$ and $Cl_{q,2^i n'}(a) + 2n'$ are disjoint sets of the same size $\mathrm{ord}_{\Theta_{2^i n'}(a)}(q)$, we have $|Cl_{q,2^i n'(a)}| = \mathrm{ord}_{\Theta_{2^{i+1}n'}(a)}(q) = 2\,\mathrm{ord}_{\Theta_{2^i n'}(a)}(q) = |Cl_{q,2^i n'}(a) \cup (Cl_{q,2^i n'}(a)+2^i n')|$. Therefore, $Cl_{q,2^{i+1}n'}(a) = Cl_{q,2^i n'}(a) \cup (Cl_{q,2^i n'}(a)+2^i n')$ as desired.

To prove (ii), assume that $\lambda > 0$. For (a), suppose that $1 \in Cl_{q,2^{\lambda+\beta-1}n'}(1+2^{\lambda+\beta-2}n')$. If $\lambda = 1$, then $\lambda+\beta-1 = \beta$, we have $\mathrm{ord}_{2^{\lambda+\beta-1}}(q) = 2 = \mathrm{ord}_{2^{\lambda+\beta-2}}(q)$ by Lemma 4. Since $2 \| \mathrm{ord}_{n'}(q)$, we have $(\mathrm{ord}_{n'}(q)/2)$ is odd and it follows that $\mathrm{ord}_{2^{\lambda+\beta-1}n'}(q) = lcm(\mathrm{ord}_{2^{\lambda+\beta-1}}(q), \mathrm{ord}_{n'}(q)) = \mathrm{lcm}(\mathrm{ord}_{2^{\lambda+\beta-2}}(q), \mathrm{ord}_{\Theta_{n'}}(a)(q)) = \mathrm{ord}_{\Theta_{2^{\lambda+\beta-2}n'}(a)}(q)$. Assume that $\lambda \geq 2$. Since $\lambda + \beta - 1 \geq \beta + 1$, we have $\text{ord}_{2^{\lambda+\beta-1}}(q) = 2^{\lambda}$ and $\text{ord}_{2^{\lambda+\beta-2}}(q) = 2^{\lambda-1}$ by Lemma 4. Since $2^{\lambda} \| \text{ord}_{n'}(q)$, it follows that

$$\begin{aligned}
\text{ord}_{2^{\lambda+\beta-1}n'}(q) &= \text{lcm}\left(\text{ord}_{2^{\lambda+\beta-1}}(q), \text{ord}_{n'}(q)\right) \\
&= \text{lcm}\left(2^{\lambda}, \text{ord}_{n'}(q)\right) \\
&= \text{lcm}\left(2^{\lambda-1}, \text{ord}_{n'}(q)\right) \\
&= \text{lcm}\left(\text{ord}_{2^{\lambda+\beta-2}}(q), \text{ord}_{n'}(q)\right) = \text{ord}_{2^{\lambda+\beta-2}n'}(q).
\end{aligned} \tag{10}$$

Since $2^{\lambda} \| \text{ord}_{n'}(q)$, $(\text{ord}_{n'}(q)/2^{\lambda})$ is odd. Hence, $\text{ord}_{2^{\lambda+\beta-1}n'}(q) = \text{lcm}(\text{ord}_{2^{\lambda+\beta-1}}(q), \text{ord}_{n'}(q)) = \text{lcm}(\text{ord}_{2^{\lambda+\beta-2}}(q), \text{ord}_{n'}(q)) = \text{ord}_{2^{\lambda+\beta-2}n'}(q)$. Since $1 + 2^{\lambda+\beta-2}n' \not\equiv 1 \pmod{2^{\lambda+\beta-1}n'}$, we have $1 + 2^{\lambda+\beta-2}n' \equiv q^j \pmod{2^{\lambda+\beta-1}n'}$ for some $0 < j < \text{ord}_{\Theta_{2^{\lambda+\beta-1}n'}(1)}(q) = \text{ord}_{2^{\lambda+\beta-1}n'}(q)$. It follows that $1 \equiv q^j \pmod{2^{\lambda+\beta-2}n'}$ which implies that $\text{ord}_{2^{\lambda+\beta-2}n'}(q) \leq j < \text{ord}_{2^{\lambda+\beta-1}n'}(q) = \text{ord}_{2^{\lambda+\beta-2}n'}(q)$, a contradiction. Therefore, $Cl_{q,2^{\lambda+\beta-1}n'}(1) \neq Cl_{q,2^{\lambda+\beta-1}n'}(1 + 2^{\lambda+\beta-2}n')$, as desired.

To prove (b), let a be an odd integer, and let i be an integer such that $i \geq \lambda + \beta - 1$. Then, $i \geq \beta$ which implies that $\text{ord}_{2^{i+1}}(q) = 2\,\text{ord}_{2^i}(q)$ and $\text{ord}_{2^i}(q) = 2^{i-\beta+1} \geq 2^{\lambda}$ by Lemma 4. Since $2^{\lambda} \| \text{ord}_{n'}(q)$, $(\text{ord}_{n'}(q)/2^{\lambda})$ is odd and

$$\begin{aligned}
\text{ord}_{2^{i+1}n'}(q) &= \text{lcm}\left(\text{ord}_{2^{i+1}}(q), \text{ord}_{n'}(q)\right) \\
&= \text{lcm}\left(2\,\text{ord}_{2^i}(q), \text{ord}_{n'}(q)\right) \\
&= \text{lcm}\left(2\,\text{ord}_{2^i}(q), \frac{\text{ord}_{n'}(q)}{2^{\lambda}}\right) \\
&= 2\,\text{lcm}\left(\text{ord}_{2^i}(q), \frac{\text{ord}_{n'}(q)}{2^{\lambda}}\right) \\
&= 2\,\text{lcm}\left(\text{ord}_{2^i}(q), \text{ord}_{n'}(q)\right) = 2\,\text{ord}_{2^i n'}(q),
\end{aligned} \tag{11}$$

which implies that $aq^{ord_{2^i n'}(q)} \not\equiv a \pmod{2^{i+1}n'}$. Since $aq^{\text{ord}_{2^i n'}(q)} \equiv a \pmod{2^i n'}$, we have $aq^{\text{ord}_{2^i n'}(q)} \equiv a + 2^i n' \pmod{2^{i+1}n'}$. Hence, $a + 2^i n' \in Cl_{q,2^{i+1}n'}(a)$ which implies that $Cl_{q,2^{i+1}n'}(a) = Cl_{q,2^{i+1}n'}(a + 2n')$. The first equality holds.

For the second equality, let $b \in Cl_{q,2^{i+1}n'}(a)$. Then, $b \equiv aq^j \pmod{2^{i+1}n'}$ for some $0 \leq j < \text{ord}_{\Theta_{2^{i+1}n'}(a)}(q)$. It follows that $b \equiv aq^j \pmod{2^i n'}$. If $b < 2^i n'$, then $b \in Cl_{q,2^i n'}(a)$. Otherwise, $b - 2^i n' \in Cl_{q,2^i n'}(a)$ which implies that $b \in Cl_{q,2^i n'}(a) + 2^i n'$. Hence, $Cl_{q,2^{i+1}n'}(a) \subseteq Cl_{q,2^i n'}(a) \cup (Cl_{q,2^i n'}(a) + 2^i n')$. Since $Cl_{q,2^i n'}(a)$ and $Cl_{q,2^i n'}(a) + 2^i n'$ are disjoint sets of the same size $\text{ord}_{\Theta_{2^i n'}(a)}(q)$, we have $|Cl_{q,2^{i+1}n'}(a)| = \text{ord}_{\Theta_{2^{i+1}n'}(a)}(q) = 2\,\text{ord}_{\Theta_{2^i n'}(a)}(q) = |Cl_{q,2^i n'}(a) \cup (Cl_{q,2^i n'}(a) + 2^i n')|$. Therefore, $Cl_{q,2^{i+1}n'}(a) = Cl_{q,2^i n'}(a) \cup (Cl_{q,2^i n'}(a) + 2^i n')$ as desired. □

3.2. $q \equiv 1$ (mod 4). Here, we investigate properties of q-cyclotomic cosets in the case where $q \equiv 1 \pmod 4$. We begin with an explicit formula for $\text{ord}_{2^i}(q)$ which can be derived from ([11], Proposition 1). For completeness, a rigorous proof is provided.

Lemma 5. *Let q be an odd prime power, and let β be the positive integer such that $2^{\beta} \| (q^2 - 1)$. Let i be a positive integer. If $q \equiv 1$ (mod 4), then*

$$\text{ord}_{2^i}(q) = \begin{cases} 1, & \text{if } 1 \leq i \leq \beta - 1, \\ 2^{i-\beta+1}, & \text{if } i \geq \beta. \end{cases} \tag{12}$$

Proof. Assume that $q \equiv 1 \pmod 4$. Then, $2^{\beta-1} \| (q - 1)$ which implies that $\text{ord}_{2^i}(q) = 1$, for all $1 \leq i \leq \beta - 1$. Next, assume that $i \geq \beta$. Since $q \equiv 1 \pmod 4$, it follows that $q^{2^j} \equiv 1 \pmod 4$ for all $j \geq 0$. Hence, $2 \| (q^{2^j} + 1)$ for all $j \geq 0$. Since $(q^{2^{i-\beta}} - 1)(q^{2^{i-\beta}} + 1) = q^{2^{i-\beta+1}} - 1 = (q - 1)\prod_{j=0}^{i-\beta}(q^{2^j} + 1)$, it can be concluded that $2^i \| (q^{2^{\beta-i+1}} - 1)$ and $2^i \nmid (q^{2^t} - 1)$, for all $t \leq \beta + i$. As desired, we have $\text{ord}_{2^i}(q) = 2^{i-\beta+1}$ for all $i \geq \beta$. □

Proposition 2. *Let q be a prime power such that $q \equiv 1$ (mod 4), and let n' be an odd positive integer such that $\gcd(q, n') = 1$. Let $\lambda \geq 0$ be the integer such that $2^{\lambda} \| ord_{n'}(q)$, and let β be the positive integer such that $2^{\beta} || (q^2 - 1)$. Then, the following statements hold:*

(i) If $\lambda = 0$, then

(a) $Cl_{q,2^{i+1}n'}(a) \neq Cl_{q,2^{i+1}n'}(a + 2^i n')$ for all odd integers a and integers $1 \leq i \leq \beta - 2$

(b) $Cl_{q,2^{i+1}n'}(a) = Cl_{q,2^{i+1}n'}(a + 2^i n') = Cl_{q,2^i n'}(a) \cup (Cl_{q,2^i n'}(a) + 2^i n')$ for all odd integers a and integers $i \geq \beta - 1$

(ii) If $\lambda > 0$, then

(a) $Cl_{q,2^{\lambda+\beta-1}n'}(1) \neq Cl_{q,2^{i\lambda+\beta-1}n'}(1 + 2^{\lambda+\beta-2}n')$

(b) $Cl_{q,2^{i+1}n'}(a) = Cl_{q,2^{i+1}n'}(a + 2^i n') = Cl_{q,2^i n'}(a) \cup (Cl_{q,2^i n'}(a) + 2^i n')$ for odd integers a and integers $i \geq \lambda + \beta - 1$

Proof. First, we observe that $\beta \geq 3$, $2 \| (q + 1)$ and $2^{\beta-1} \| (q - 1)$. Using Lemma 5 and arguments similar to those in the proof of Proposition 1, the following key results can be deduced:

(1) If $\lambda = 0$, then $\text{ord}_{\Theta_{2^{i+1}n'}(a)}(q) = \text{ord}_{\Theta_{2^i n'}(a)}(q)$, for all odd integers a and integers $1 \leq i \leq \beta - 2$, and $\text{ord}_{2^{i+1}n'}(q) = 2\,\text{ord}_{2^i n'}(q)$, for all integers $i \geq \beta - 1$.

(2) If $\lambda > 0$, then $\text{ord}_{2^{\lambda+\beta-1}n'}(q) = \text{ord}_{2^{\lambda+\beta-2}n'}(q)$ and $\text{ord}_{2^{i+1}n'}(q) = 2\,\text{ord}_{2^i n'}(q)$, for all integers $i \geq \lambda + \beta - 1$.

The complete proof can be obtained using arguments similar to those in Proposition 1, while the above discussion and Lemma 5 is applied instead of Lemma 4. □

4. Factorization of $x^n + 1$ over Finite Fields

In this section, the factorization of $x^{2^i n'} + 1$ over $\mathbb{F}_q$ is established. First, we prove that there exists a positive integer k such that the number of monic irreducible factors of $x^{2^i n'} + 1$ over $\mathbb{F}_q$ becomes a constant for all integers $i \geq k$. In the case where $\mathrm{ord}_{n'}(q)$ is odd, a complete recursive factorization of $x^{2^i n'} + 1$ over $\mathbb{F}_q$ is given together with a recursive formula for the number of its monic irreducible factors for all positive integers i in Section 4.1. In the case where $\mathrm{ord}_{n'}(q)$ is even, a recursive factorization of $x^{2^i n'} + 1$ over $\mathbb{F}_q$ is given as well as a recursive formula for the number of its monic irreducible factors for all integers $i \geq k$ in Section 4.2.

4.1. Recursive Factorization of $x^n + 1$ over $\mathbb{F}_q$ with Odd $ord_{n'}(q)$.

In this section, we establish a complete recursive factorization of $x^{2^i n'} + 1$ over $\mathbb{F}_q$ in the case where $\mathrm{ord}_{n'}(q)$ is odd. Subsequently, a formula for the number of monic irreducible factors of $x^{2^i n'} + 1$ over $\mathbb{F}_q$ is given recursively on i.

4.1.1. $q \equiv 3 \ (mod\, 4)$.

We begin with useful relations between q-cyclotomic cosets and their induced polynomials for the case $q \equiv 3 \ (\mathrm{mod}\, 4)$.

Lemma 6. *Let q be a prime power such that $q \equiv 3 \ (mod\, 4)$, and let n' be an odd positive integer such that $gcd(q, n') = 1$ and $ord_{n'}(q)$ is odd. Let β be the positive integer such that $2^\beta \| (q^2 - 1)$.* Let i be a positive integer, and let a be an odd integer. Then, one of the following statements holds:

(i) $Cl_{q,2^{i+1}n'}(a)$ and $Cl_{q,2^{i+1}n'}(a + 2^i n')$ induce distinct monic irreducible polynomials of degree $|Cl_{q,2^i n'}(a)|$, for all $2 \leq i \leq \beta - 1$.

(ii) For each $i = 1$ or $i \geq \beta$, if $f(x)$ is induced by $Cl_{q,2^i n'}(a)$, then $Cl_{q,2^i n'}(a)$ induces $f(x^2)$.

Proof. To prove (i), assume that $2 \leq i \leq \beta - 1$. By Proposition 1 ((a) in (i)), we have $Cl_{q,2^{i+1}n'}(a) \neq Cl_{q,2^{i+1}n'}(a + 2^i n')$. From Lemma 3, it follows that $|Cl_{q,2^{i+1}n'}(a)| = |Cl_{q,2^{i+1}n'}(a + 2^i n')|$ which equals to $|Cl_{q,2^i n'}(a)|$ by the proof of Proposition 1 ((a) in (i)). Hence, $Cl_{q,2^{i+1}n'}(a)$ and $Cl_{q,2^{i+1}n'}(a + 2^i n')$ induce distinct monic irreducible polynomials of degree $|Cl_{q,2^i n'}(a)|$.

To prove (ii), assume that $i = 1$ or $i \geq \beta$. Assume that $f(x)$ is induced by $Cl_{q,2^i n'}(a)$. Let α be a $2^{i+1}n'$th root of unity. Then, α^2 is a $2^i n'$ th root of unity and $f(x) = \prod_{j \in Cl_{q,2^i n'}(a)} (x - (\alpha^2)^j)$. From Proposition 1 ((b) in (i)), we have $Cl_{q,2^{i+1}n'}(a) = Cl_{q,2^i n'}(a) \cup (Cl_{q,2^i n'}(a) + 2^i n')$. It follows that

$$
\begin{aligned}
\prod_{j \in Cl_{q,2^{i+1}n'}(a)} \left(x - \alpha^j\right) &= \prod_{j \in Cl_{q,2^i n'}(a) \cup \left\{Cl_{q,2^i n'}(a) + 2^i n'\right\}} \left(x - \alpha^j\right), \\
&= \prod_{j \in Cl_{q,2^i n'}(a)} \left(x - \alpha^j\right) \times \prod_{j \in \left\{Cl_{q,2^i n'}(a) + 2^i n'\right\}} \left(x - \alpha^j\right) \\
&= \prod_{j \in Cl_{q,2^i n'}(a)} \left(x - \alpha^j\right)\left(x - \alpha^{j + 2^i n'}\right) \\
&= \prod_{j \in Cl_{q,2^i n'}(a)} \left(x - \alpha^j\right)\left(x + \alpha^j\right) \\
&= \prod_{j \in Cl_{q,2^i n'}(a)} \left(x - \alpha^{2j}\right) \\
&= f\left(x^2\right).
\end{aligned}
\tag{13}
$$

Therefore, $Cl_{q,2^{i+1}n'}(a)$ induces $f(x^2)$ as desired. □

The next corollary can be deduced directly from the above lemma.

Corollary 1. *Assume the notations as in Lemma 6 with $i \geq \beta$. If $f(x)$ is induced by $Cl_{q,2^i n'}(a)$, then $f(x^{2^j})$ is irreducible for all $j \geq \beta - i$.*

In order to simplify the notations in the following theorem, let α and γ be $2^i n'$th and $2^{i+1}n'$th roots of unity, respectively. For each $a \in \mathrm{SO}_q(2^i n')$, let

$$
\begin{aligned}
f_a(x) &= \prod_{j \in Cl_{q,2^i n'}(a)} \left(x - \alpha^j\right) \text{ and} \\
g_j(x) &= \prod_{j \in Cl_{q,2^{i+1}n'}(a)} \left(x - \gamma^j\right).
\end{aligned}
\tag{14}
$$

be the irreducible polynomials induced by $Cl_{q,2^i n'}(a)$ and $Cl_{q,2^{i+1}n'}(a)$, respectively. Using these notations, a recursive factorization of $x^{2^i n'}+1$ is given as follows.

Theorem 1. *Let q be a prime power such that $q \equiv 3 \ (mod\, 4)$, and let n' be an odd positive integer such that $gcd(q,n')=1$ and $ord_{n'}(q)$ is odd. Let β be the positive integer such that $2^\beta \| (q^2-1)$. Then, the following statements hold:*

(i) If $i=0$, then

$$x^{2^i n'}+1 = x^{n'}+1 = \prod_{a\in SO_q(2n')} f_a(x). \tag{15}$$

(ii) If $i \geq 1$, then

$$x^{2^i n'}+1 = \begin{cases} \prod\limits_{a\in SO_q(2^i n')} f_a(x^2), & \text{if } i=1 \text{ or } i\geq\beta, \\ \prod\limits_{a\in SO_q(2^i n')} g_a(x) g_{a+2^i n'}(x), & \text{if } 2\leq i\leq \beta-1, \end{cases} \tag{16}$$

where $f_a(x)$ and $g_a(x)$ are given in (14).

In this case, we have

$$x^{2^{\beta-1+i}n'}+1 = \prod_{a\in SO_q(2^\beta n')} f_a\left(x^{2^i}\right), \tag{17}$$

for all $i\geq 0$.

Proof. From (5), we note that

$$x^{2^i n'}+1 = \prod_{a\in SO_q(2^{i+1}n')} f_a(x). \tag{18}$$

The first statement is the special case where $i=0$. From Proposition 1 (i), it can be deduced that

$$SO_q\left(2^{i+1}n'\right) = \begin{cases} SO_q\left(2^i n'\right), & \text{if } i=1 \text{ or } i\geq\beta, \\ SO_q\left(2^i n'\right)\cup\left(SO_q\left(2^i n'\right)+2^i n'\right), & \text{if } 2\leq i\leq\beta-1, \end{cases} \tag{19}$$

where the union is disjoint. The results therefore follow from Lemma 6. □

A recursive formula for the number of monic irreducible factors of $x^{2^i n'}+1$ over $\mathbb{F}_q$ follows immediately from the theorem.

Corollary 2. *Let q be a prime power such that $q\equiv 3\ (mod\, 4)$, and let n' be an odd positive integer such that $gcd(q,n')=1$ and $ord_{n'}(q)$ is odd. Let $i\geq 0$ be an integer, and let β be the positive integer such that $2^\beta\|(q^2-1)$. Then,*

$$N_q(n') = \sum_{d|n'} \frac{\phi(2d)}{\mathrm{ord}_{2d}(q)}, \tag{20}$$

$$N_q\left(2^i n'\right) = \begin{cases} N_q(n') & \text{if } i=1, \\ 2N_q\left(2^{i-1}n'\right) = 2^{i-1}N_q(n') & \text{if } 2\leq i\leq\beta-1, \\ N_q\left(2^{\beta-2}n'\right) = 2^{\beta-2}N_q(n') & \text{if } i\geq\beta. \end{cases} \tag{21}$$

Proof. Equation (20) is a special case of (6). Equation (21) follows immediately from Theorem 1. □

4.1.2. $q\equiv 1\ (mod\, 4)$. Here, we focus on $q\equiv 1 \ (\mathrm{mod}\, 4)$. First, some useful relations between the q-cyclotomic coset $Cl_{q,2^{i+1}n'}(a)$ and its induced polynomial are established.

Lemma 7. *Let q be a prime power such that $q\equiv 1\ (mod\, 4)$, and let n' be an odd positive integer such that $gcd(q,n')=1$ and $ord_{n'}(q)$ is odd. Let β be the positive integer such that $2^\beta\|(q^2-1)$. Let i be a positive integer, and let a be an odd integer. Then, one of the following statements holds:*

(i) $Cl_{q,2^{i+1}n'}(a)$ and $Cl_{q,2^{i+1}n'}(a+2^i n')$ induce distinct monic irreducible polynomials of the same degree for all $1\leq i\leq\beta-2$

(ii) For each $i\geq\beta-1$, if $f(x)$ is induced by $Cl_{q,2^i n'}(a)$, then $Cl_{q,2^{i+1}n'}(a)$ induces $f(x^2)$

Proof. The proof can be obtained using arguments similar to those in the proof of Lemma 6, while Proposition 2 (i) is applied instead of Proposition 1 (i). □

Corollary 3. *Assume the notations as in Lemma 7 with $i\geq\beta-1$.* If $f(x)$ is induced by $Cl_{q,2^i n'}(a)$, then $f(x^{2^j})$ is irreducible for all $j\geq\beta-i-1$.

The factorization of $x^{2^i n'}+1$ is given in the following theorem.

Theorem 2. *Let q be a prime power such that $q\equiv 1\ (mod\, 4)$, and let n' be an odd positive integer such that $gcd(q,n')=1$ and $ord_{n'}(q)$ is odd. Let β be the positive integer such that $2^\beta\|(q^2-1)$. Then, the following statements hold:*

(i) If $i=0$, then

$$x^{2^i n'}+1 = x^{n'}+1 = \prod_{a\in SO_q(2n')} f_a(x). \tag{22}$$

(ii) If $i\geq 1$, then

$$x^{2^i n'}+1=\begin{cases}\prod_{a\in SO_q(2^i n')} g_a(x)g_{a+2^i n'}(x), & \text{if } 1\le i\le \beta-2,\\ \prod_{a\in SO_q(2^i n')} f_a\left(x^2\right), & \text{if } i\ge \beta-1,\end{cases} \tag{23}$$

where $f_a(x)$ and $g_a(x)$ are given in (14).

In this case, we have

$$x^{2^{\beta-2+i}n'}+1=\prod_{a\in SO_q(2^{\beta-1}n')} f_a\left(x^{2^i}\right), \tag{24}$$

for all $i\ge 0$.

Proof. The proof can be obtained using arguments similar to those in the proof of Theorem 1, while Proposition 2 (i) and Lemma 7 are applied instead of Proposition 1 (i) and Lemma 6. □

From the theorem, the enumeration of monic irreducible factors of $x^{2^i n'}-1$ over $\mathbb{F}_q$ can be concluded in the following corollary.

Corollary 4. *Let q be a prime power such that $q\equiv 1\ (mod\, 4)$, and let n' be an odd positive integer such that $gcd(q,n')=1$ and $ord_{n'}(q)$ is odd. Let $i\ge 0$ be an integer, and let β be the positive integer such that $2^\beta \| (q^2-1)$. Then,*

$$N_q(n')=\sum_{d|n'}\frac{\phi(2d)}{\mathrm{ord}_{2d}(q)}, \tag{25}$$

$$N_q\left(2^i n'\right)=\begin{cases}2N_q\left(2^{i-1}n'\right)=2^iN_q(n'), & \text{if } 1\le i\le\beta-2,\\ N_q\left(2^{\beta-2}n'\right)=2^{\beta-2}N_q(n'), & \text{if } i\ge\beta-1.\end{cases} \tag{26}$$

Proof. Equation (25) is given in (6). Equation (26) follows immediately from Theorem 2. □

4.2. Factorization of x^n+1 over $\mathbb{F}_q$ with Even $ord_{n'}(q)$. In this section, we focus on the case where $\mathrm{ord}_{n'}(q)$ is even, i.e., $2^\lambda \| \mathrm{ord}_{n'}(q)$ for some positive integer λ. The results are not strong as the previous section. Precisely, a recursive factorization of $x^{2^i n'}+1$ over $\mathbb{F}_q$ is given only for all sufficiently large positive integers i.

In general, the factorization of $x^{2^i n'}+1$ over $\mathbb{F}_q$ is given in (3). For $i\ge\lambda+\beta-1$, a simpler recursive method for the factorization is given in the following theorem.

Theorem 3. *Let q be an odd prime power, and let n' be an odd positive integer such that $gcd(q,n')=1$. Let λ be the positive integer such that $2^\lambda \| ord_{n'}(q)$, and let β be the positive integer such that $2^\beta \| (q^2-1)$. Then,*

$$x^{2^{\lambda+\beta-1+j}n'}+1=\prod_{a\in SO_q(2^{\lambda+\beta}n')} f_a\left(x^{2^j}\right), \tag{27}$$

for all $j\ge 0$.

Proof. The proof can be obtained using arguments similar to those in the proof of Theorem 1, while Proposition 2 (ii) and Proposition 1 (ii) are applied instead of Proposition 2 (i) and Proposition 1 (i). □

Corollary 5 follows immediately.

Corollary 5. *Let q be an odd prime power, and let n' be an odd positive integer such that $gcd(q,n')=1$. Let λ be the positive integer such that $2^\lambda \| ord_{n'}(q)$, and let β be the positive integer such that $2^\beta \| (q^2-1)$. Then,*

$$N_q\left(2^i n'\right)=N_q\left(2^{\lambda+\beta-2}n'\right), \tag{28}$$

for all $i\ge\lambda+\beta-1$.

4.3. Algorithm and Examples. In this section, the above results are summarized as an algorithm for factorizing $x^{2^i n'}+1$ over $\mathbb{F}_q$. Some illustrative examples are given as well. An algorithm for the factorization of $x^{2^i n'}+1$ over $\mathbb{F}_q$ is given in Algorithm 1.

Note that $f_a(x)$ and $g_a(x)$ are given in (14).

For the enumeration of monic irreducible factors of $x^{2^i n'}+1$ over $\mathbb{F}_q$, it can be calculated using (6). With more information on n', i, and q, the formula can be simplified using Corollaries 2, 4, and 5 of the form

$$N_q\left(2^i n'\right)=\begin{cases}2^iN_q(n'), & \text{if } \lambda=0,\ 1\le i\le\beta-2 \text{ and } q\equiv 1\ (\mathrm{mod}\, 4),\\ 2^{\beta-2}N_q(n'), & \text{if } \lambda=0,\ i\ge\beta-1 \text{ and } q\equiv 1\ (\mathrm{mod}\, 4),\\ N_q(n'), & \text{if } \lambda=0,\ i=1 \text{ and } q\equiv 3\ (\mathrm{mod}\, 4),\\ 2^{i-1}N_q(n'), & \text{if } \lambda=0,\ 2\le i\le\beta-1 \text{ and } q\equiv 3\ (\mathrm{mod}\, 4),\\ 2^{\beta-2}N_q(n'), & \text{if } \lambda=0,\ i\ge\beta \text{ and } q\equiv 3\ (\mathrm{mod}\, 4),\\ N_q\left(2^{\lambda+\beta-2}n'\right), & \text{if } \lambda\ge 1 \text{ and } i\ge\lambda+\beta-1,\end{cases} \tag{29}$$

Input: odd prime power q, odd integer n' with $\gcd(q,n')=1$, and integer $i\geq 0$.
(1) Compute the positive integer β such that $2^{\beta}\|(q^2-1)$.
(2) Compute $\mathrm{ord}_{n'}(q)$ and the integer λ such that $2^{\lambda}\|\mathrm{ord}_{n'}(q)$.
(3) Consider the following cases:

(I) $\lambda=0$.

(i) $q\equiv 1 \pmod 4$.

(a) $i=0$. Compute $x^{2^i n'}+1=x^{n'}+1=\prod_{a\in \mathrm{SO}_q(2n')} f_a(x)$.
(b) $1\leq i\leq \beta-2$. Compute
$x^{2^i n'}+1=\prod_{a\in \mathrm{SO}_q(2^i n')} g_a(x) g_{a+2^i n'}(x)$,
and $\mathrm{SO}_q(2^{i+1}n')=\mathrm{SO}_q(2^i n')\cup(\mathrm{SO}_q(2^i n')+2^i n')$.
(c) $i\geq\beta-1$. Compute
$x^{2^i n'}+1=\prod_{a\in \mathrm{SO}_q(2^{\beta-1}n')} f_a(x^{2^{i-\beta+2}})$.

(ii) $q\equiv 3 \pmod 4$.

(a) $0\leq i\leq 1$. Compute $x^{2^i n'}+1=\prod_{a\in SO_q(2n')} f_a(x^i)$.
(b) $2\leq i\leq\beta-1$. Compute
$x^{2^i n'}+1=\prod_{a\in \mathrm{SO}_q(2^i n')} g_a(x) g_{a+2^i n'}(x)$,
and $\mathrm{SO}_q(2^{i+1}n')=\mathrm{SO}_q(2^i n')\cup(\mathrm{SO}_q(2^i n')+2^i n')$.
(c) $i\geq\beta$. Compute
$x^{2^i n'}+1=\prod_{a\in \mathrm{SO}_q(2^{\beta}n')} f_a(x^{2^{i-\beta+1}})$.

(II) $\lambda\geq 1$.

(i) $0\leq i\leq\lambda+\beta-2$. Compute $x^{2^i n'}+1$ directly using (3)
(ii) $i\geq\lambda+\beta-1$. Compute

$x^{2^i n'}+1=\prod_{a\in \mathrm{SO}_q(2^{\lambda+\beta}n')} f_a(x^{2^{i-\lambda-\beta+1}})$.

ALGORITHM 1: Algorithm for the factorization of $x^{2^i n'}+1$ over Fq.

where λ is the positive integer such that $2^{\lambda}\|\mathrm{ord}_{n'}(q)$, β is the positive integer such that $2^{\beta}\|(q^2-1)$, and

$$N_q(n')=\sum_{d|n'}\frac{\phi(2d)}{\mathrm{ord}_{2d}(q)}. \tag{30}$$

From (29), the number $N_q(2^i n')$ of monic irreducible factors of $x^{2^i n'}+1$ over $\mathbb{F}_q$ becomes a constant independent of i for all $i\geq\lambda+\beta-1$ if $\lambda=0$ and $q\equiv 3 \pmod 4$ and for all $i\geq\lambda+\beta-2$ otherwise. Illustrative examples for the number $N_q(2^i n')$ of monic irreducible factors of $x^{2^i n'}+1$ over $\mathbb{F}_q$ with odd $\mathrm{ord}_{n'}(q)$ and even $\mathrm{ord}_{n'}(q)$ are given in Tables 1 and 2, respectively.

In Table 1, the results for $q\in\{3,7\}$ and $q\in\{5,9\}$ are obtained from Corollaries 2 and 4, respectively.

In Table 2, the last row of each n' is obtained from Corollary 5. Otherwise, it is computed using (6).

5. Applications

In this section, the factorization of $x^{2^i n'}+1$ over $\mathbb{F}_q$ obtained in Section 4 is applied in the study of negacyclic codes. Some known results are revisited in simpler forms.

A linear code of length n over $\mathbb{F}_q$ is defined to be a subspace of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$. The *dual* of a linear code C of length n over $\mathbb{F}_q$ is defined to be

$$C^{\perp}=\left\{(v_0,v_1,\ldots,v_{n-1})\in\mathbb{F}_q^n \mid \sum_{i=0}^{n-1}c_i v_i=0,\quad \text{for all } (c_0,c_1,\ldots,c_{n-1})\in C\right\}. \tag{31}$$

A linear code C is said to be *self-dual* if $C=C^{\perp}$ and it is said to be complementary dual if $C\cap C^{\perp}=\{0\}$.

A linear code C of length n over $\mathbb{F}_q$ is said to be negacyclic if it is closed under the negacyclic shift. Precisely, $(-c_{n-1},c_0,c_1,\ldots,c_{n-2})\in C$, for every $(c_0,c_1,\ldots,c_{n-2},c_{n-1})\in C$. Under the map π: $\mathbb{F}_q^n\longrightarrow(\mathbb{F}_q[x]/\langle x^n+1\rangle)$ defined by

$$(c_0,c_1,\ldots,c_{n-2},c_{n-1})\mapsto c_0+c_1x+c_2x^2+\cdots+c_{n-1}x^{n-1}, \tag{32}$$

it is well known (see [4]) that a linear code C of length n over $\mathbb{F}_q$ is negacyclic if and only if $\pi(C)$ is an ideal in the principal ideal ring $(\mathbb{F}_q[x]/\langle x^n+1\rangle)$. The map π induces a one-to-one correspondence between negacyclic codes of length n over $\mathbb{F}_q$ and ideas in $(\mathbb{F}_q[x]/\langle x^n+1\rangle)$. In this case, $\pi(C)$ is uniquely generated by the monic divisor of x^n+1 of minimal degree in $\pi(C)$. Such polynomial is called the *generator polynomial* of C.

Let q be an odd prime power, and let n' be an odd positive integer such that $\gcd(q,n')=1$. Let λ be the positive

TABLE 1: $N_q(2^i n')$ of monic irreducible factors of $x^{2^i n'}+1$ over $\mathbb{F}_q$ with odd $\mathrm{ord}_{n'}(q)$.

q	n'	$\mathrm{ord}_{n'}(q)$	λ	β	i	$N_q(2^i n')$
3	1	1	0	3	0	1
					1	1
					≥ 2	2
3	11	5	0	3	0	3
					1	3
					≥ 2	6
3	13	3	0	3	0	5
					1	5
					≥ 2	10
5	1	1	0	3	0	1
					≥ 1	2
5	11	5	0	3	0	3
					≥ 1	6
7	1	1	0	4	0	1
					1	1
					2	2
					≥ 3	4
7	3	1	0	4	0	3
					1	3
					2	6
					≥ 3	12
7	9	3	0	4	0	5
					1	5
					2	10
					≥ 3	20
9	1	1	0	4	0	1
					1	2
					≥ 2	4
9	7	3	0	4	0	3
					1	6
					≥ 2	12
9	11	5	0	4	0	3
					1	6
					≥ 2	12
9	13	3	0	4	0	5
					1	10
					≥ 2	20

TABLE 2: $N_q(2^i n')$ of monic irreducible factors of $x^{2^i n'}+1$ over $\mathbb{F}_q$ with even $\mathrm{ord}_{n'}(q)$.

q	n'	$\mathrm{ord}_{n'}(q)$	λ	β	i	$N_q(2^i n')$
3	5	4	2	3	0	2
					1	3
					2	6
					≥ 3	10
3	7	6	1	3	0	2
					1	3
					≥ 2	6
5	3	2	1	3	0	2
					1	4
					≥ 2	6
5	7	6	1	3	0	2
					1	4
					≥ 2	6
5	9	6	1	3	0	3
					1	6
					≥ 2	10
5	13	4	2	3	0	4
					1	8
					2	14
					≥ 3	26
7	5	4	2	4	0	2
					1	3
					2	6
					3	12
					≥ 4	20
7	11	10	1	4	0	2
					1	3
					2	6
					≥ 3	12
7	13	12	2	4	0	2
					1	3
					2	6
					3	12
					≥ 4	20
7	15	4	2	4	0	6
					1	9
					2	18
					3	36
					≥ 4	60
9	5	2	1	4	0	3
					1	6
					2	12
					≥ 3	20

integer such that $2^\lambda \| \mathrm{ord}_{n'}(q)$, and let β be the positive integer such that $2^\beta \| (q^2-1)$. Let

$$k = \begin{cases} \lambda+\beta-1, & \text{if } \lambda = 0 \text{ and } q \equiv 3 \pmod 4, \\ \lambda+\beta-2, & \text{otherwise.} \end{cases} \tag{33}$$

In general, negacyclic codes have been studied in [3, 4, 10]. Here, we focus on negacyclic codes of length $n = p^s 2^i n'$ with $i \geq k$, where p is the characteristic of $\mathbb{F}_q$. The construction and enumeration of such negacyclic codes are simplified using the results from Section 4.

From (5), we have

$$x^{2^k n'} + 1 = \prod_{j=1}^{N_q(2^k n')} r_j(x). \tag{34}$$

Based on Theorems 1–3, it follows that

$$x^{p^s 2^i n'} + 1 = \left(x^{2^i n'} + 1\right)^{p^s} = \prod_{j=1}^{N_q(2^k n')} \left(r_j\left(x^{2^{i-k}}\right)\right)^{p^s}, \tag{35}$$

and $r_j(x^{2^{i-k}})$ is irreducible for all $i \geq k$.

The following characterization and enumeration of negacyclic codes of length $n = p^s 2^i n'$ with $i \geq k$ are straightforward. The proof is committed.

Theorem 4. *Assume the notations above. The following statements hold:*

(1) *The map* $T\colon (\mathbb{F}_q[x]/\langle x^{p^s 2^k n'}+1\rangle) \longrightarrow (\mathbb{F}_q[x]/\langle x^{p^s 2^i n'}+1\rangle)$, *defined by* $f(x)\mapsto f(x^{2^{i-k}})$, *is a ring isomorphism for all integers* $i\geq k$

(2) *For each integer* $i\geq k$, $g(x)$ *is the generator polynomial of a negacyclic code of length* p^s2^kn' *over* $\mathbb{F}_q$ *if and only if* $g(x^{2^{i-k}})$*is the generator polynomial of a negacyclic code of length* p^s2^in' *over* $\mathbb{F}_q$

(3) *The number of negacyclic codes of length* p^s2^in' *over* $\mathbb{F}_q$ *is* $(p^s+1)^{N_q(2^kn')}$, *for all* $i\geq k$

From the theorem, all negacyclic codes of length p^s2^in' over $\mathbb{F}_q$ with $i\geq k$ can be determined using the negacyclic codes of length p^s2^kn' over $\mathbb{F}_q$.

Data Availability

No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

S. Jitman was supported by the Thailand Research Fund under Research Grant RSA6280042.

References

[1] G. K. Bakshi and M. Raka, "Self-dual and self-orthogonal negacyclic codes of length $2p^n$ over a finite field," *Finite Fields and Their Applications*, vol. 19, pp. 39–54, 2013.

[2] T. Blackford, "Negacyclic duadic codes," *Finite Fields and Their Applications*, vol. 14, no. 4, pp. 930–943, 2008.

[3] S. Jitman, S. Prugsapitak, S. Prugsapitak, and M. Raka, "Some generalizations of good integers and their applications in the study of self-dual negacyclic codes," *Advances in Mathematics of Communications*, vol. 14, no. 1, pp. 35–51, 2020.

[4] E. Sangwisut, S. Jitman, S. Ling, and P. Udomkavanich, "Hulls of cyclic and negacyclic codes over finite fields," *Finite Fields and Their Applications*, vol. 33, pp. 232–257, 2015.

[5] Y. Wu, Q. Yue, and S. Fan, "Self-reciprocal and self-conjugate-reciprocal irreducible factors of $x^n-\lambda$ and their applications," *Finite Fields and Their Applications*, vol. 63, Article ID 101648, 2020.

[6] Y. Jia, S. Ling, and C. Xing, "On self-dual cyclic codes over finite fields," *IEEE Transactions on Information Theory*, vol. 57, pp. 2243–2251, 2011.

[7] I. F. Blake, S. Gao, and R. C. Mullin, "Explicit factorization of $x^{2^k}-1$ over F_p with prime $p\equiv 3 \bmod 4$," *Applicable Algebra in Engineering, Communication and Computing*, vol. 4, no. 2, pp. 89–94, 1993.

[8] H. Meyn, "Factorization of the cyclotomic Polynomial $x^{2^n}+1$ over finite fields," *Finite Fields and Their Applications*, vol. 2, no. 4, pp. 439–442, 1996.

[9] S. Ling and C. Xing, *Coding Theory: A First Course*, Cambridge University Press, Cambridge, UK, 2004.

[10] A. Boripan and S. Jitman, "SRIM and SCRIM factors of x^n+1 over finite fields and their applications,"*Discrete Mathematics, Algorithms and Applications*.

[11] F. R. Beyl, "Cyclic subgroups of the prime residue group," *The American Mathematical Monthly*, vol. 84, no. 1, pp. 46–48, 1977.