AIMS Mathematics, 11(9): 29327–29364.
DOI: 10.3934/math.20261166
Received: 05 May 2026
Revised: 02 September 2026
Accepted: 07 September 2026
Published: 11 September 2026

https://www.aimspress.com/journal/Math

Research article

An alternative perspective on recursive factorization of $x^n - 1$ over finite fields and applications in coding theory

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:** Email: sjitman@gmail.com; Tel: +66897378538.

Abstract: Building on the well-known factorization of $x^n - 1$ over finite fields $\mathbb{F}_q$, this paper presents an alternative perspective on its irreducible factors in arithmetic settings where they admit explicit recursive descriptions. As applications, these results are used in the characterization and enumeration of self-orthogonal cyclic codes over finite fields. We first consider the case $n = p^s$, where p is an odd prime coprime to q, and show that suitable irreducible factors can be obtained recursively by power substitutions from factors at a critical degree. This recursive viewpoint is then extended to a product of two odd prime powers and, more generally, to certain finite products of distinct odd prime powers under suitable separation conditions on multiplicative orders. From these recursive descriptions, we derive explicit formulas for the numbers of monic irreducible factors of $x^n - 1$ over $\mathbb{F}_q$. We then apply the same framework to the study of self-reciprocal irreducible monic and self-conjugate-reciprocal irreducible monic factors of $x^n - 1$. In particular, we obtain structural descriptions in extremal cases where all irreducible factors are of the corresponding type or where $x - 1$ is the unique such factor. These results are further applied to the enumeration of Euclidean and Hermitian self-orthogonal cyclic codes. In this way, the paper provides an explicit recursive and enumerative framework connecting the factorization patterns of $x^n - 1$ with counting problems and constructions in algebraic coding theory.

Keywords: recursive factorization; cyclotomic cosets; self-reciprocal irreducible monic polynomials; self-conjugate-reciprocal irreducible monic polynomials; Euclidean inner product; Hermitian inner product; self-orthogonal cyclic codes
Mathematics Subject Classification: 12E20, 94B15, 94B60

1. Introduction

The factorization of $x^n - 1$ over a finite field $\mathbb{F}_q$ is a fundamental tool in the study of the cyclic codes and related classes of linear codes. Since cyclic codes of length n over $\mathbb{F}_q$ correspond to ideals of the quotient ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$, their algebraic structure is determined by the irreducible factors of $x^n - 1$ over $\mathbb{F}_q$ [1, 2]. In particular, such factorizations play an important role in the study of cyclic codes and their duals; see, for example, [3–6]. For this reason, it is useful to understand not only the irreducible factors themselves but also their recursive behavior, their enumeration, and their interaction with reciprocal and conjugate-reciprocal operations. The factorization of $x^n - 1$ over finite fields is classical and well known, both in direct and recursive forms (see, for example, [2, 7, 8]). The point of view adopted in this paper is different. We focus on alternative recursive factorization patterns that arise under explicit arithmetic conditions. In these cases, the factorization at higher prime power levels can be obtained from that at suitable critical levels by simple power substitutions. This leads to a structured description which is particularly convenient for enumeration problems in coding theory.

In many cases, especially when n contains a prime power divisor satisfying certain arithmetic conditions, the factorization of $x^n - 1$ exhibits a recursive structure. A simple example occurs over $\mathbb{F}_3$, where

$$x^5 - 1 = (x - 1)f(x),$$
$$x^{5^2} - 1 = (x - 1)f(x)f(x^5),$$

and

$$x^{5^3} - 1 = (x - 1)f(x)f(x^5)f(x^{5^2}),$$

with

$$f(x) = x^4 + x^3 + x^2 + x + 1.$$

Later, in Corollary 3.2, we prove that

$$x^{5^s} - 1 = (x - 1)\prod_{j=0}^{s-1} f(x^{5^j})$$

for all $s \geq 1$. This example suggests that once the factorization at a suitable critical degree is known, the factorizations at higher degrees may be obtained recursively through substitutions of the form $x \mapsto x^{p^j}$.

The behavior of reciprocal factors of $x^n - 1$ is closely related to the arithmetic of multiplicative orders. Self-reciprocal irreducible monic (SRIM) factors have been used in the classification and enumeration of self-dual, self-orthogonal codes, complementary dual codes, and hulls of codes with respect to the Euclidean inner product; see, for instance, [3, 6, 9]. In the Hermitian setting, self-conjugate-reciprocal irreducible monic (SCRIM) factors provide an analogous role over $\mathbb{F}_{q^2}$ and have been studied in connection with Hermitian duality including self-dual codes, self-orthogonal codes, complementary dual codes, and hulls of codes; see, for example, [5, 10]. These are also connected with the theory of good integers and related divisibility conditions involving expressions of the form $a^k + b^k$, which have appeared in both number theory and coding theory [11–13].

The first aim of this paper is to give an alternative perspective on the recursive factorization of $x^n - 1$ over finite fields. We begin with the prime power case $n = p^s$, where p is an odd prime not dividing q,

and explain that the irreducible factors induced by certain q-cyclotomic cosets are obtained by power substitutions of x. We then extend this description to an odd integer $n = p_1^{s_1} p_2^{s_2}$ and, more generally, to some finite products of odd prime powers coprime to q. This yields explicit factorization patterns that reduce the problem of factoring $x^n - 1$ at higher degrees to the determination of irreducible factors at a suitable critical degree. On the basis of the recursive factorization results, we derive explicit formulas for the number of monic irreducible factors of $x^n - 1$ in case of the prime power and some finite products of prime powers. This recursive viewpoint is particularly useful in coding theory. For cyclic codes, the factorization of $x^n - 1$ determines the possible generator polynomials, and hence the structure of the codes themselves. In particular, the recursive framework developed here provides a systematic way to derive formulas for the numbers of irreducible, SRIM, and SCRIM factors of $x^n - 1$, which forms the basis of the second aim of this paper.

The second aim is to apply these results to SRIM and SCRIM factors of $x^n - 1$ over finite fields. More precisely, we study SRIM factors over $\mathbb{F}_q$ and SCRIM factors over $\mathbb{F}_{q^2}$ in the same framework. We obtain descriptions in the extremal situations where all irreducible factors are SRIM or SCRIM, and where $x - 1$ is the unique such factor. Furthermore, these enumerative results have direct applications to coding theory. The distributions of irreducible, SRIM, and SCRIM factors lead naturally to enumeration formulas for Euclidean and Hermitian self-orthogonal cyclic codes.

The third aim is to connect these factorization results with applications in coding theory. The distributions of SRIM and SCRIM factors are used to enumerate Euclidean and Hermitian self-orthogonal cyclic codes.

The paper is organized as follows. In Section 2, we recall the basic definitions concerning multiplicative orders, q-cyclotomic cosets, and irreducible factors of $x^n - 1$. Section 3 is devoted to alternative recursive factorizations in the prime power and some finite product of prime powers, together with explicit factorization templates. In Section 4, formulas for the numbers of monic irreducible factors are obtained and then applied to the enumeration of SRIM and SCRIM factors. In Section 5, the results from earlier sections are applied to the enumeration of Euclidean and Hermitian self-orthogonal cyclic codes over finite fields. Finally, Section 6 summarizes the main results and indicates possible directions for further investigation.

2. Preliminaries

For a prime p and a positive integer a, the notation $p^s \parallel a$ means that s is the largest non-negative integer such that p^s divides a. Equivalently, $p^s \mid a$ but $p^{s+1} \nmid a$. In this case, s is called the *p-adic valuation of a* and it is denoted by $\nu_p(a) = s$. For positive integers i and j with $\gcd(i, j) = 1$, the *multiplicative order of j modulo i*, denoted by $\mathrm{ord}_i(j)$, is the smallest positive integer s such that $j^s \equiv 1 \pmod{i}$.

For an integer a and a positive integer n with $\gcd(n, q) = 1$, the *q-cyclotomic coset modulo n containing a* is defined by

$$\mathrm{Cl}_{q,n}(a) = \{aq^j \bmod n : j = 0, 1, \dots\}.$$

It is easily seen that

$$|\mathrm{Cl}_{q,n}(a)| = \mathrm{ord}_{n/\gcd(n,a)}(q).$$

Let ζ be a primitive n-th root of unity in a suitable extension field of $\mathbb{F}_q$. For each integer a, define

$$f_a(x) = \prod_{i \in \mathrm{Cl}_{q,n}(a)} (x - \zeta^i).$$

Then $f_a(x)$ is a monic irreducible polynomial over $\mathbb{F}_q$. Moreover, $f_a(x) = f_b(x)$ if and only if $\mathrm{Cl}_{q,n}(a) = \mathrm{Cl}_{q,n}(b)$. Let Γ be a complete set of representatives of the distinct q-cyclotomic cosets modulo n. From [2], the factorization of $x^n - 1$ over $\mathbb{F}_q$ is given by

$$x^n - 1 = \prod_{a \in \Gamma} f_a(x).$$

The following standard results will be used frequently.

Theorem 2.1. *([14, Theorem 3.6]) Let q be a prime power and let p be an odd prime such that $\gcd(p, q) = 1$. Let γ be the positive integer such that $p^\gamma \parallel (q^{\mathrm{ord}_p(q)} - 1)$. Then, for every positive integer s, we have*

$$\mathrm{ord}_{p^s}(q) = \begin{cases} \mathrm{ord}_p(q), & \text{if } 1 \le s \le \gamma, \\ \mathrm{ord}_p(q) p^{s-\gamma}, & \text{if } s > \gamma. \end{cases}$$

The recursive factorization results in Section 3 are established only for odd prime power components, since they rely on the lifting formula for $\mathrm{ord}_{p^s}(q)$ in Theorem 2.1.

Lemma 2.2. *Let q be a prime power and let p be an odd prime such that $\gcd(p, q) = 1$. Let a be a positive integer such that $\gcd(a, p) = 1$, and let γ be the positive integer satisfying $p^\gamma \parallel (q^{\mathrm{ord}_p(q)} - 1)$. Then, for $0 \le i < s$, the size of the q-cyclotomic coset $\mathrm{Cl}_{q,p^s}(ap^i)$ is*

$$|\mathrm{Cl}_{q,p^s}(ap^i)| = \begin{cases} \mathrm{ord}_p(q) p^{s-i-\gamma}, & \text{if } s - i > \gamma, \\ \mathrm{ord}_p(q), & \text{if } s - i \le \gamma. \end{cases}$$

Proof. Let m be the smallest positive integer such that

$$ap^i q^m \equiv ap^i \pmod{p^s}.$$

This congruence is equivalent to $p^s \mid ap^i(q^m - 1)$. Since $\gcd(a, p) = 1$, this is equivalent to $p^{s-i} \mid (q^m - 1)$, or, equivalently

$$q^m \equiv 1 \pmod{p^{s-i}}.$$

Therefore,

$$|\mathrm{Cl}_{q,p^s}(ap^i)| = \mathrm{ord}_{p^{s-i}}(q).$$

The result now follows directly from Theorem 2.1. Indeed, if $s - i \le \gamma$, then

$$\mathrm{ord}_{p^{s-i}}(q) = \mathrm{ord}_p(q),$$

whereas if $s - i > \gamma$, then

$$\mathrm{ord}_{p^{s-i}}(q) = \mathrm{ord}_p(q) p^{s-i-\gamma}.$$

This proves the lemma. □

3. Recursive factorization of $x^n - 1$ over finite fields

In this section, we present recursive patterns in the factorization of $x^n - 1$ over $\mathbb{F}_q$. The main idea is that, under suitable arithmetic conditions, irreducible factors at higher degrees can be obtained from factors at a lower critical degree by power substitutions. However, as pointed out by one of the referees, the classical procedure already suggests a recursive behavior (see Remarks 3.3 and 3.10). Therefore, the purpose of our formulation is to give an alternative recursive view and make this recursive structure explicit at the level of irreducible factors and q-cyclotomic cosets, and then to use it systematically in enumeration problems and coding-theoretic applications.

We first treat the odd prime power case $n = p^s$, then extend the result to a product of two prime powers, and finally discuss the corresponding extension to a finite product of distinct prime powers.

3.1. The case of prime power

We begin with the case $n = p^s$, where p is an odd prime not dividing q. The recursive structure in this case is determined by the largest power of p dividing $q^{\mathrm{ord}_p(q)} - 1$. More precisely, if

$$p^\gamma \parallel (q^{\mathrm{ord}_p(q)} - 1),$$

then, by Theorem 2.1, the order $\mathrm{ord}_{p^s}(q)$ remains constant up to the critical level p^γ and then grows by a factor of p at each subsequent level. The parameter γ is obtained by first computing $d = \mathrm{ord}_p(q)$ and then determining

$$\gamma = \nu_p(q^d - 1) = \nu_p(q^{\mathrm{ord}_p(q)} - 1).$$

This classical lifting behavior leads directly to a recursive description of the irreducible factors of $x^{p^s} - 1$. We present the resulting prime power recursion in our notation, since it provides the basic recursive form used in the subsequent analysis of products of distinct odd prime powers.

Theorem 3.1. *Let q be a prime power, let p be an odd prime such that $\gcd(p, q) = 1$, and let γ be the positive integer such that $p^\gamma \parallel (q^{\mathrm{ord}_p(q)} - 1)$. If s is a positive integer such that $s \geq \gamma$, then*

$$f_{ap^i}(x) = f_{ap^{s-\gamma}}(x^{p^{s-\gamma-i}})$$

for every positive integer a such that $\gcd(a, p) = 1$ and every $i \in \{0, 1, \ldots, s-\gamma\}$, where $f_{ap^i}(x)$ denotes the irreducible factor induced by the q-cyclotomic coset $\mathrm{Cl}_{q,p^s}(ap^i)$.

Proof. Let ζ be a primitive p^s-th root of unity in a suitable extension field of $\mathbb{F}_q$. Then, $f_{ap^i}(x)$ is the minimal polynomial of ζ^{ap^i} over $\mathbb{F}_q$.

Fix $i \in \{0, 1, \ldots, s-\gamma\}$ and set $r = s - \gamma - i$. Since

$$(\zeta^{ap^i})^{p^r} = \zeta^{ap^{s-\gamma}},$$

the element ζ^{ap^i} is a root of

$$f_{ap^{s-\gamma}}(x^{p^r}).$$

Hence, by the minimality of $f_{ap^i}(x)$, we have

$$f_{ap^i}(x) \mid f_{ap^{s-\gamma}}(x^{p^r}).$$

By Lemma 2.2 and Theorem 2.1

$$\deg(f_{ap^i}(x)) = p^{s-\gamma-i}\,\mathrm{ord}_p(q) = p^r\,\mathrm{ord}_p(q),$$

while $\deg(f_{ap^{s-\gamma}}(x)) = \mathrm{ord}_p(q)$. Therefore

$$\deg(f_{ap^{s-\gamma}}(x^{p^r})) = p^r\,\mathrm{ord}_p(q) = \deg(f_{ap^i}(x)).$$

Since both polynomials are monic, the divisibility above and equality of degrees imply

$$f_{ap^i}(x) = f_{ap^{s-\gamma}}(x^{p^{s-\gamma-i}}).$$

This proves the result. □

By Theorem 3.1, the factors corresponding to $a, ap, ap^2, \ldots, ap^{s-\gamma}$ are recursively generated from the factor $f_{ap^{s-\gamma}}(x)$ through the substitutions $x \mapsto x^{p^{s-\gamma}}, x \mapsto x^{p^{s-\gamma-1}}, x \mapsto x^{p^{s-\gamma-2}}, \ldots, x \mapsto x$. Equivalently

$$\begin{aligned}
f_a(x) &= f_{ap^{s-\gamma}}(x^{p^{s-\gamma}}),\\
f_{ap}(x) &= f_{ap^{s-\gamma}}(x^{p^{s-\gamma-1}}),\\
f_{ap^2}(x) &= f_{ap^{s-\gamma}}(x^{p^{s-\gamma-2}}),\\
&\vdots\\
f_{ap^{s-\gamma-1}}(x) &= f_{ap^{s-\gamma}}(x^{p}),\\
f_{ap^{s-\gamma}}(x) &= f_{ap^{s-\gamma}}(x).
\end{aligned}$$

A practical description of the full factorization of $x^{p^s} - 1$ can be recursively deduced on the basis of Theorem 3.1 once the factorization at the critical degree p^γ is known.

Corollary 3.2. *Let q be a prime power and let p be an odd prime such that $\gcd(p, q) = 1$. Let $p^\gamma \parallel (q^{\mathrm{ord}_p(q)} - 1)$. Assume that the factorization of $x^{p^\gamma} - 1$ over $\mathbb{F}_q$ is*

$$x^{p^\gamma} - 1 = (x-1)f_1(x)f_2(x)\cdots f_r(x),$$

where $f_1(x), f_2(x), \ldots, f_k(x)$ are precisely the irreducible factors among $f_1(x), f_2(x), \ldots, f_r(x)$ that divide $x^{p^{\gamma-1}} - 1$. Then, for every $s \geq \gamma$, we have

$$x^{p^s} - 1 = (x-1)\prod_{i=1}^{k} f_i(x) \prod_{j=0}^{s-\gamma}\prod_{i=k+1}^{r} f_i(x^{p^j}).$$

Proof. Since the factors $f_1(x), f_2(x), \ldots, f_k(x)$ already occur at degree $p^{\gamma-1}$, they remain unchanged in the factorization of $x^{p^s} - 1$. The remaining factors are those appearing for the first time at the critical degree p^γ. By Theorem 3.1, each such factor generates the chain

$$f_i(x),\ f_i(x^p),\ f_i(x^{p^2}),\ \ldots,\ f_i(x^{p^{s-\gamma}}).$$

Combining the stable factors and these generated chains gives the stated factorization. □

Remark 3.3. *Building on the classical factorization of x^n-1 over finite fields $\mathbb{F}_q$ (see, for example, [8]), one may consider the cyclotomic decomposition*

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

where $\Phi_d(x)$ denotes the d-th cyclotomic polynomial. Thus, the factorization of x^n-1 over $\mathbb{F}_q$ is reduced to factoring each $\Phi_d(x)$ over $\mathbb{F}_q$. Equivalently, for each divisor d of n, one may choose a primitive d-th root of unity ξ_d in a suitable extension field of $\mathbb{F}_q$ and compute its minimal polynomial over $\mathbb{F}_q$. The distinct irreducible factors then correspond to the q-cyclotomic cosets modulo d in the unit group of $\mathbb{Z}_d$.

In the prime power case $n = p^s$, where p is an odd prime with $p \nmid q$, this standard procedure may be expressed in a recursive form as follows:

(1) Let $d = \mathrm{ord}_p(q)$. Then there exists an extension field K of $\mathbb{F}_q$ of degree d containing a primitive p-th root of unity. If β is a generator of the multiplicative group $K^\times$, then

$$\zeta_p = \beta^{(q^d-1)/p}$$

is a primitive p-th root of unity in K. The minimal polynomial of ζ_p over $\mathbb{F}_q$ gives an irreducible factor of $\Phi_p(x)$ over $\mathbb{F}_q$.

(2) Let

$$\gamma = \nu_p(q^{\mathrm{ord}_p(q)} - 1).$$

Then $p^\gamma \parallel (q^d - 1)$ and γ is the critical exponent determining the highest level before the recursive power substitution pattern begins. Starting from a primitive p-th root of unity, one may determine primitive p^j-th roots of unity for $1 \le j \le \gamma$ and compute their minimal polynomials over $\mathbb{F}_q$. In this way, one obtains the irreducible factors corresponding to

$$\Phi_p(x), \Phi_{p^2}(x), \ldots, \Phi_{p^\gamma}(x).$$

(3) For $m > \gamma$, once a minimal polynomial $\mu_\gamma(x)$ of a primitive p^γ-th root of unity is known, the corresponding minimal polynomial of a primitive p^m-th root of unity is obtained by

$$\mu_m(x) = \mu_\gamma(x^{p^{m-\gamma}}).$$

In our formulation, this is precisely the recursive pattern made explicit in Theorem 3.1 and Corollary 3.2. After the critical level p^γ, the higher p-power factors are generated recursively by power substitutions.

Example 3.4. *Consider the factorization of $x^{3^7}-1$ over $\mathbb{F}_{53}$. Since $\mathrm{ord}_3(53) = 2$ and $3^3 \parallel (53^{\mathrm{ord}_3(53)}-1)$, we have $\gamma = 3$. Hence, the critical degree is $3^\gamma = 3^3$.*

First, we note that the factorization of $x^{3^2} - 1$ over $\mathbb{F}_{53}$ is

$$x^{3^2} - 1 = (x-1) \prod_{c\in\{1,18,39,49\}} (x^2 + cx + 1),$$

and the factorization of $x^{3^3} - 1$ over $\mathbb{F}_{53}$ is

$$x^{3^3} - 1 = (x-1) \prod_{c\in\{1,18,39,49\}} (x^2 + cx + 1) \prod_{d\in\{3,6,12,17,19,30,31,46,48\}} (x^2 + dx + 1).$$

By Corollary 3.2, the factorization of $x^{3^7} - 1$ *over* $\mathbb{F}_{53}$ *is*

$$x^{3^7} - 1 = (x-1) \prod_{c \in \{1,18,39,49\}} (x^2 + cx + 1) \prod_{j=0}^{4} \left(\prod_{d \in \{3,6,12,17,19,30,31,46,48\}} \left(x^{2 \cdot 3^j} + dx^{3^j} + 1 \right) \right).$$

3.2. The case of the product of two odd prime powers

In this subsection, we consider an alternative recursive factorization of $x^n - 1$ over $\mathbb{F}_q$ in the case

$$n = p_1^{s_1} p_2^{s_2},$$

where p_1 and p_2 are distinct odd primes not dividing q. In contrast to the case of prime power, the behavior of the q-cyclotomic cosets depends on the interaction between the two prime power components.

The main new theoretical contribution of our recursive framework begins in this setting. We determine a precise arithmetic separation criterion under which the multiplicative order modulo $p_1^{s_1} p_2^{s_2}$ splits into independent prime power contributions. Under this criterion, the associated q-cyclotomic cosets admit a uniform recursive block structure, which leads to the recursive factorization in Theorem 3.6. The same principle is subsequently extended to certain finite products of distinct odd prime powers.

The following lemma gives the exact arithmetic condition required for this multiplicative order separation and hence for the recursive factorization argument.

Lemma 3.5. *Let q be a prime power and p_1 and p_2 be distinct odd primes such that* $\gcd(p_1 p_2, q) = 1$. *For $t = 1, 2$, let $d_t = \mathrm{ord}_{p_t}(q)$ and $p_t^{\gamma_t} \parallel (q^{d_t} - 1)$. Assume that $s_t \geq \gamma_t$ for $t = 1, 2$. Then,*

$$\mathrm{ord}_{p_1^{s_1} p_2^{s_2}}(q) = p_1^{s_1 - \gamma_1} p_2^{s_2 - \gamma_2} \, \mathrm{lcm}(d_1, d_2) \tag{3.1}$$

if and only if

$$s_1 = \gamma_1 \text{ or } p_1 \nmid d_2, \quad \text{and} \quad s_2 = \gamma_2 \text{ or } p_2 \nmid d_1.$$

In particular, if $s_1 > \gamma_1$ and $s_2 > \gamma_2$, then (3.1) *holds if and only if $p_1 \nmid d_2$ and $p_2 \nmid d_1$.*

Proof. Since p_1 and p_2 are distinct primes and $\gcd(p_1 p_2, q) = 1$, we have

$$\mathrm{ord}_{p_1^{s_1} p_2^{s_2}}(q) = \mathrm{lcm}(\mathrm{ord}_{p_1^{s_1}}(q), \mathrm{ord}_{p_2^{s_2}}(q)).$$

By Theorem 2.1, $\mathrm{ord}_{p_t^{s_t}}(q) = d_t p_t^{s_t - \gamma_t}$ for all $t = 1, 2$. Consequently,

$$\mathrm{ord}_{p_1^{s_1} p_2^{s_2}}(q) = \mathrm{lcm}(d_1 p_1^{s_1 - \gamma_1}, d_2 p_2^{s_2 - \gamma_2}).$$

Set $A = s_1 - \gamma_1$ and $B = s_2 - \gamma_2$. Since $d_1 = \mathrm{ord}_{p_1}(q)$ divides $p_1 - 1$, we have $p_1 \nmid d_1$. Similarly, $p_2 \nmid d_2$. Comparing the p_1-adic valuations, we obtain

$$\nu_{p_1} \left(\mathrm{lcm}(d_1 p_1^A, d_2 p_2^B) \right) = \max\{A, \nu_{p_1}(d_2)\},$$

whereas

$$\nu_{p_1} \left(p_1^A p_2^B \, \mathrm{lcm}(d_1, d_2) \right) = A + \nu_{p_1}(d_2).$$

These two quantities are equal if and only if $A = 0$ or $\nu_{p_1}(d_2) = 0$. Equivalently, $s_1 = \gamma_1$ or $p_1 \nmid d_2$.

Similarly, comparing the p_2-adic valuations gives that equality holds if and only if $s_2 = \gamma_2$ or $p_2 \nmid d_1$. Therefore,

$$\operatorname{lcm}(d_1 p_1^{s_1-\gamma_1}, d_2 p_2^{s_2-\gamma_2}) = p_1^{s_1-\gamma_1} p_2^{s_2-\gamma_2} \operatorname{lcm}(d_1, d_2),$$

if and only if $s_1 = \gamma_1$ or $p_1 \nmid d_2$, and $s_2 = \gamma_2$ or $p_2 \nmid d_1$. The result follows. □

Under the separation criterion established in Lemma 3.5, the classical prime power recursion extends to the product of two distinct odd prime powers. This yields the following recursive factorization result, which is one of the main theoretical contributions.

Theorem 3.6. *Let q be a prime power and p_1 and p_2 be distinct odd primes such that* $\gcd(p_1 p_2, q) = 1$. *For $t = 1, 2$, let $d_t = \operatorname{ord}_{p_t}(q)$ and $p_t^{\gamma_t} \parallel (q^{d_t} - 1)$ and let s_t be an integer such that $s_t \geq \gamma_t$. Assume that $s_1 = \gamma_1$ or $p_1 \nmid d_2$, and $s_2 = \gamma_2$ or $p_2 \nmid d_1$. Let a be a positive integer such that* $\gcd(a, p_1 p_2) = 1$. *Then,*

$$f_{ap_1^{i_1} p_2^{i_2}}(x) = f_{ap_1^{s_1-\gamma_1} p_2^{s_2-\gamma_2}}\left(x^{p_1^{s_1-\gamma_1-i_1} p_2^{s_2-\gamma_2-i_2}}\right),$$

for all $0 \leq i_1 \leq s_1 - \gamma_1$ and $0 \leq i_2 \leq s_2 - \gamma_2$, where $f_{ap_1^{i_1} p_2^{i_2}}(x)$ is induced by the q-cyclotomic coset $\mathrm{Cl}_{q, p_1^{s_1} p_2^{s_2}}(ap_1^{i_1} p_2^{i_2})$.

Proof. By Lemma 3.5, we have

$$\operatorname{ord}_{p_1^{s_1} p_2^{s_2}}(q) = p_1^{s_1-\gamma_1} p_2^{s_2-\gamma_2} \operatorname{lcm}(d_1, d_2).$$

Let α be a primitive element of $\mathbb{F}_{q^{p_1^{s_1-\gamma_1} p_2^{s_2-\gamma_2} \operatorname{lcm}(d_1,d_2)}}$ and set

$$j = \frac{q^{p_1^{s_1-\gamma_1} p_2^{s_2-\gamma_2} \operatorname{lcm}(d_1,d_2)} - 1}{p_1^{s_1} p_2^{s_2}}.$$

Then, α^j is a primitive $p_1^{s_1} p_2^{s_2}$-th root of unity. The q-cyclotomic coset $\mathrm{Cl}_{q, p_1^{s_1} p_2^{s_2}}(ap_1^{i_1} p_2^{i_2})$ has a size

$$p_1^{s_1-\gamma_1-i_1} p_2^{s_2-\gamma_2-i_2} \operatorname{lcm}(d_1, d_2) = \operatorname{ord}_{p_1^{s_1-i_1} p_2^{s_2-i_2}}(q),$$

by Lemma 3.5. Since $0 \leq i_t \leq s_t - \gamma_t$, we have $s_t - i_t \geq \gamma_t$ for all $t = 1, 2$. It follows that the coset can be partitioned into $\operatorname{lcm}(d_1, d_2)$ subsets

$$C_m = \left\{ ap_1^{i_1} p_2^{i_2} q^{r \operatorname{lcm}(d_1,d_2)+m} \bmod p_1^{s_1} p_2^{s_2} : 0 \leq r < p_1^{s_1-\gamma_1-i_1} p_2^{s_2-\gamma_2-i_2} \right\},$$

where $0 \leq m \leq \operatorname{lcm}(d_1, d_2) - 1$. For each $k \in C_m$, we obtain

$$((\alpha^j)^k)^{p_1^{s_1-\gamma_1-i_1} p_2^{s_2-\gamma_2-i_2}} = (\alpha^j)^{ap_1^{s_1-\gamma_1} p_2^{s_2-\gamma_2} q^{r \operatorname{lcm}(d_1,d_2)+m}} = \left((\alpha^j)^{ap_1^{s_1-\gamma_1} p_2^{s_2-\gamma_2} q^m}\right)^{q^{r \operatorname{lcm}(d_1,d_2)}}.$$

Since $p_t^{\gamma_t} \mid (q^{d_t} - 1)$ and $d_t \mid \operatorname{lcm}(d_1, d_2)$ for $t = 1, 2$, it follows that

$$p_1^{\gamma_1} p_2^{\gamma_2} \mid (q^{\operatorname{lcm}(d_1,d_2)} - 1).$$

Hence, the power $q^{\mathrm{lcm}(d_1,d_2)}$ fixes every root of unity whose order divides $p_1^{\gamma_1}p_2^{\gamma_2}$. Therefore,

$$((\alpha^j)^k)^{p_1^{s_1-\gamma_1-i_1}p_2^{s_2-\gamma_2-i_2}} = (\alpha^j)^{ap_1^{s_1-\gamma_1}p_2^{s_2-\gamma_2}q^m}.$$

Consequently,

$$\prod_{k\in C_m}(x-(\alpha^j)^k) = x^{p_1^{s_1-\gamma_1-i_1}p_2^{s_2-\gamma_2-i_2}} - (\alpha^j)^{ap_1^{s_1-\gamma_1}p_2^{s_2-\gamma_2}q^m}.$$

Multiplying over $0 \le m \le \mathrm{lcm}(d_1,d_2)-1$, we obtain

$$f_{ap_1^{i_1}p_2^{i_2}}(x) = f_{ap_1^{s_1-\gamma_1}p_2^{s_2-\gamma_2}}\left(x^{p_1^{s_1-\gamma_1-i_1}p_2^{s_2-\gamma_2-i_2}}\right).$$

This proves the result. □

Under certain conditions, a pattern similar to that of the case of odd prime power is obtained for the case of a product of two odd prime powers, as shown by Theorem 3.6. Once the factor

$$f_{ap_1^{s_1-\gamma_1}p_2^{s_2-\gamma_2}}(x)$$

is known, the preceding factors are obtained by the substitutions

$$x \mapsto x^{p_1^{u_1}p_2^{u_2}},$$

where $0 \le u_t \le s_t - \gamma_t$ for $t = 1, 2$. Thus, the recursive structure is indexed by a two-dimensional grid rather than by a single chain.

Corollary 3.7. *Let q be a prime power, and let p_1 and p_2 be distinct odd primes such that $\gcd(p_1p_2, q) = 1$. For $t = 1, 2$, let $d_t = \mathrm{ord}_{p_t}(q)$ and let γ_t be the positive integer such that $p_t^{\gamma_t} \parallel (q^{d_t}-1)$. Let $s_t \ge \gamma_t$ and assume that $s_1 = \gamma_1$ or $p_1 \nmid d_2$, and $s_2 = \gamma_2$ or $p_2 \nmid d_1$. Set*

$$n_0 = p_1^{\gamma_1}p_2^{\gamma_2},$$

and let

$$x^{n_0} - 1 = \prod_{f\in\mathcal{F}_0} f(x)$$

be its factorization into monic irreducible factors over $\mathbb{F}_q$. For each $f \in \mathcal{F}_0$, let $p_1^{e_1(f)}p_2^{e_2(f)}$ be the common multiplicative order of the roots of f, where $0 \le e_t(f) \le \gamma_t$. Define

$$\begin{aligned}
\mathcal{F}_\varnothing &= \{f \in \mathcal{F}_0 : e_1(f) < \gamma_1,\ e_2(f) < \gamma_2\},\\
\mathcal{F}_1 &= \{f \in \mathcal{F}_0 : e_1(f) = \gamma_1,\ e_2(f) < \gamma_2\},\\
\mathcal{F}_2 &= \{f \in \mathcal{F}_0 : e_1(f) < \gamma_1,\ e_2(f) = \gamma_2\},\\
\mathcal{F}_{12} &= \{f \in \mathcal{F}_0 : e_1(f) = \gamma_1,\ e_2(f) = \gamma_2\}.
\end{aligned}$$

Then, we have

$$x^{p_1^{s_1}p_2^{s_2}} - 1 = \prod_{f\in\mathcal{F}_\varnothing} f(x) \times \prod_{f\in\mathcal{F}_1}\prod_{j_1=0}^{s_1-\gamma_1} f\left(x^{p_1^{j_1}}\right) \times \prod_{f\in\mathcal{F}_2}\prod_{j_2=0}^{s_2-\gamma_2} f\left(x^{p_2^{j_2}}\right) \times \prod_{f\in\mathcal{F}_{12}}\prod_{j_1=0}^{s_1-\gamma_1}\prod_{j_2=0}^{s_2-\gamma_2} f\left(x^{p_1^{j_1}p_2^{j_2}}\right).$$

Proof. Let $g(x)$ be an irreducible factor of $x^{p_1^{s_1}p_2^{s_2}}-1$, and let ξ be a root of $g(x)$. Write the multiplicative order of ξ as $p_1^{r_1}p_2^{r_2}$ for $0 \le r_t \le s_t$. Set $e_t = \min\{r_t, \gamma_t\}$, $j_t = \max\{r_t - \gamma_t, 0\}$, and $M = p_1^{j_1}p_2^{j_2}$. Then ξ^M has the order $p_1^{e_1}p_2^{e_2}$, and hence ξ^M is a root of a unique factor $f(x) \in \mathcal{F}_0$. Therefore, ξ is a root of $f(x^M)$ which implies that $g(x) \mid f(x^M)$.

It remains to compare their degrees. Indeed, by Theorem 2.1, $\mathrm{ord}_{p_t^{r_t}}(q) = p_t^{j_t}\,\mathrm{ord}_{p_t^{e_t}}(q)$ for all $t = 1, 2$. Since $e_t \le \gamma_t$, we have $\mathrm{ord}_{p_t^{e_t}}(q) = d_t$ whenever $e_t \ge 1$, while $\mathrm{ord}_1(q) = 1$ if $e_t = 0$. Moreover, if $j_1 > 0$, then $s_1 > \gamma_1$ and hence $p_1 \nmid d_2$. Similarly, if $j_2 > 0$, then $p_2 \nmid d_1$. Therefore,

$$\mathrm{ord}_{p_1^{r_1}p_2^{r_2}}(q) = p_1^{j_1}p_2^{j_2}\,\mathrm{ord}_{p_1^{e_1}p_2^{e_2}}(q).$$

Consequently,

$$\deg(g(x)) = M\deg(f(x)) = \deg(f(x^M)).$$

Since both polynomials are monic, it follows that $g(x) = f(x^M)$.

If $e_1 < \gamma_1$ and $e_2 < \gamma_2$, then $j_1 = j_2 = 0$ and $f \in \mathcal{F}_\varnothing$. If $e_1 = \gamma_1$ and $e_2 < \gamma_2$, then $f \in \mathcal{F}_1$ and only powers of p_1 occur in M. The case $f \in \mathcal{F}_2$ is analogous. Finally, if $e_1 = \gamma_1$ and $e_2 = \gamma_2$, then $f \in \mathcal{F}_{12}$ and both powers may occur.

On the other hand, the same degree argument shows that each polynomial displayed in these four families is an irreducible factor of $x^{p_1^{s_1}p_2^{s_2}}-1$. Moreover, the order of its roots uniquely determines j_1 and j_2, while the corresponding factor f at the critical level is unique. Hence, the four families are pairwise disjoint and together give the stated factorization. □

3.3. The case of the product of finite odd prime powers

Finally, we briefly extend the preceding recursive factorization to a finite product of distinct odd prime powers. The same idea applies when the prime power components separate uniformly. To explain this condition more concretely, note that for

$$n = \prod_{t=1}^{\lambda} p_t^{s_t},$$

the recursive factorization argument requires the multiplicative order $\mathrm{ord}_n(q)$ to separate into two parts: A lifted prime power contribution

$$\prod_{t=1}^{\lambda} p_t^{s_t-\gamma_t}$$

and a base term $\mathrm{lcm}(d_1, \ldots, d_\lambda)$, where $d_t = \mathrm{ord}_{p_t}(q)$. The separation condition ensures that when one passes from the critical exponent γ_t to a higher exponent s_t, no additional divisibility coming from another prime p_v enters the order through d_t. In other words, each prime power component contributes independently to the lifted part of the order. This independence is exactly what allows the associated q-cyclotomic cosets to decompose into uniform blocks and hence makes the recursive power substitution argument possible. Without this condition, the prime power components may interact inside the multiplicative order, so the clean block structure of the cosets may break down. The statements below are direct analog of the corresponding results for a product of two odd prime powers, and their proofs follow by similar arguments. We therefore omit the details.

For each $t \in \{1, 2, \ldots, \lambda\}$, let $d_t = \mathrm{ord}_{p_t}(q)$ and $p_t^{\gamma_t} \parallel (q^{d_t} - 1)$. By Theorem 2.1, whenever $s_t \geq \gamma_t$, one has

$$\mathrm{ord}_{p_t^{s_t}}(q) = d_t p_t^{s_t - \gamma_t}.$$

Hence

$$\mathrm{ord}_{\prod_{t=1}^{\lambda} p_t^{s_t}}(q) = \mathrm{lcm}\left(d_1 p_1^{s_1-\gamma_1}, \ldots, d_\lambda p_\lambda^{s_\lambda - \gamma_\lambda}\right).$$

Thus, in order to obtain the separated form

$$\mathrm{ord}_{\prod_{t=1}^{\lambda} p_t^{s_t}}(q) = \left(\prod_{t=1}^{\lambda} p_t^{s_t-\gamma_t}\right)\mathrm{lcm}(d_1, \ldots, d_\lambda),$$

it is necessary and sufficient that, for every $v \in \{1, 2, \ldots, \lambda\}$ we have

$$s_v = \gamma_v \text{ or } p_v \nmid d_t \quad \text{for all} \quad t \neq v.$$

Equivalently, whenever the p_v-power is lifted beyond the critical degree γ_v, the prime p_v must not occur in any of the base orders d_t with $t \neq v$.

Under this separation condition, the q-cyclotomic cosets decompose into uniform blocks, exactly as in the case of two prime powers. Raising the roots in each block to the appropriate power collapses the block to a single root corresponding to the terminal coset. This yields the following extension.

Theorem 3.8. *Let q be a prime power and let*

$$n = \prod_{t=1}^{\lambda} p_t^{s_t},$$

where $p_1, p_2, \ldots, p_\lambda$ are distinct odd primes and $\gcd(n, q) = 1$. For each $t \in \{1, 2, \ldots, \lambda\}$, let $d_t = \mathrm{ord}_{p_t}(q)$ and $p_t^{\gamma_t} \parallel (q^{d_t} - 1)$. Assume that $s_t \geq \gamma_t$ for all, t and that, for every $v \in \{1, \ldots, \lambda\}$,

$$s_v = \gamma_v \text{ or } p_v \nmid d_t \quad \text{for all} \quad t \neq v.$$

Let a be a positive integer such that $\gcd\left(a, \prod_{t=1}^{\lambda} p_t\right) = 1$. Then,

$$f_{a\prod_{t=1}^{\lambda} p_t^{i_t}}(x) = f_{a\prod_{t=1}^{\lambda} p_t^{s_t-\gamma_t}}\left(x^{\prod_{t=1}^{\lambda} p_t^{s_t-\gamma_t-i_t}}\right),$$

where $0 \leq i_t \leq s_t - \gamma_t$ for all $t = 1, \ldots, \lambda$, and $f_{a\prod_{t=1}^{\lambda} p_t^{i_t}}(x)$ is induced by the q-cyclotomic coset $\mathrm{Cl}_{q,n}\left(a\prod_{t=1}^{\lambda} p_t^{i_t}\right)$.

The full factorization at the critical degree can be extended recursively by lifting each irreducible factor only in the prime power directions in which its root order reaches the corresponding critical exponent. Under the separation assumptions above, these liftings are independent. This yields the following full recursive factorization.

Corollary 3.9. *Let q be a prime power and let*

$$n = \prod_{t=1}^{\lambda} p_t^{s_t},$$

where $p_1, p_2, \ldots, p_\lambda$ are distinct odd primes such that $\gcd(n, q) = 1$. *For each $t \in \{1, 2, \ldots, \lambda\}$, let $d_t = \mathrm{ord}_{p_t}(q)$ and let γ_t be the positive integer such that $p_t^{\gamma_t} \parallel (q^{d_t} - 1)$. Assume that $s_t \geq \gamma_t$ for all t and that, for every $v \in \{1, 2, \ldots, \lambda\}$, $s_v = \gamma_v$, or $p_v \nmid d_t$ for all $t \neq v$. Set*

$$n_0 = \prod_{t=1}^{\lambda} p_t^{\gamma_t},$$

and let

$$x^{n_0} - 1 = \prod_{f \in \mathcal{F}_0} f(x)$$

be its factorization into monic irreducible factors over $\mathbb{F}_q$.

For each $f \in \mathcal{F}_0$, let the common multiplicative order of its roots be

$$\prod_{t=1}^{\lambda} p_t^{e_t(f)}, \qquad 0 \leq e_t(f) \leq \gamma_t,$$

and define $J(f) = \{\, t \in \{1, 2, \ldots, \lambda\} : e_t(f) = \gamma_t \,\}$. Then,

$$x^n - 1 = \prod_{f \in \mathcal{F}_0} \prod_{\substack{(j_t)_{t \in J(f)} \\ 0 \leq j_t \leq s_t - \gamma_t}} f\left(x^{\prod_{t \in J(f)} p_t^{j_t}}\right),$$

where, if $J(f) = \emptyset$, the corresponding contribution is understood to be simply $f(x)$.

For completeness, the corresponding classical viewpoint (see, for example, [8]) in the general finite product setting is reviewed in the following remark.

Remark 3.10. *Remark 3.3 extends naturally to a general positive integer*

$$n = \prod_{i=1}^{r} p_i^{m_i},$$

where the values of p_i are distinct primes and $\gcd(n, q) = 1$. *For each prime power divisor $p_i^{m_i}$, one may first determine the corresponding irreducible factors of*

$$\Phi_{p_i}(x), \Phi_{p_i^2}(x), \ldots, \Phi_{p_i^{m_i}}(x)$$

by the classical procedure described in Remark 3.3. Equivalently, one may work in suitable extension fields containing primitive $p_i^{m_i}$-th roots of unity and compute the associated minimal polynomials over $\mathbb{F}_q$.

If K_i is an extension field of $\mathbb{F}_q$ containing the relevant primitive $p_i^{m_i}$-th roots of unity, then its degree is determined by the corresponding multiplicative orders. Since finite extensions of $\mathbb{F}_q$ are determined uniquely, up to isomorphism, by their degrees, it is convenient to work inside a common extension field L of $\mathbb{F}_q$ whose degree is a common multiple of the relevant orders. In this field, primitive d-th roots of unity for divisors $d \mid n$ may be obtained as products of the roots of appropriate prime power orders, and their minimal polynomials then yield the irreducible factors of $x^n - 1$ over $\mathbb{F}_q$.

Thus, in the general case, the classical procedure produces the full factorization by assembling the prime power contributions inside a common extension field. The point of our formulation is that in suitable arithmetic settings such as those of Theorem 3.8 and Corollary 3.9, this construction can be reorganized into an explicit recursive description.

4. SRIM and SCRIM factors of $x^n - 1$

In this section, we present a systematic treatment of the numbers of monic irreducible, SRIM, and SCRIM factors of $x^n - 1$ over finite fields, based on the recursive factorizations established in Section 3. We note that direct enumerations of SRIM and SCRIM factors of $x^n - 1$ were previously discussed in [9, 10]. The importance of our results lies in the fact that they place these enumerations into a recursive framework, showing that the factorization and counting problems at higher degrees can be reduced to those at a suitable critical degree.

Let $f(x) \in \mathbb{F}_q[x]$ be a monic polynomial with a nonzero constant term. The *reciprocal polynomial* of $f(x)$ is defined by

$$f^*(x) = x^{\deg(f)} f(0)^{-1} f(x^{-1}).$$

The polynomial $f(x)$ is called self-reciprocal if $f^*(x) = f(x)$. A monic irreducible polynomial over $\mathbb{F}_q$ is called *a SRIM* polynomial if it is self-reciprocal.

Let n be a positive integer such that $\gcd(n, q) = 1$, and let ζ be a primitive n-th root of unity in an extension field of $\mathbb{F}_q$. For each integer a, we recall that the irreducible factor of $x^n - 1$ induced by the q-cyclotomic coset $\mathrm{Cl}_{q,n}(a)$ is

$$f_a(x) = \prod_{i \in \mathrm{Cl}_{q,n}(a)} (x - \zeta^i).$$

The reciprocal polynomial $f_a^*(x)$ is induced by the coset $\mathrm{Cl}_{q,n}(-a)$. Hence $f_a(x)$ is SRIM if and only if

$$\mathrm{Cl}_{q,n}(a) = \mathrm{Cl}_{q,n}(-a).$$

Equivalently, $f_a(x)$ is SRIM if and only if there exists a non-negative integer j such that $aq^j \equiv -a \pmod{n}$. In terms of the reduction modulo $\frac{n}{\gcd(n,a)}$, this is equivalent to

$$q^j \equiv -1 \pmod{\frac{n}{\gcd(n, a)}}.$$

Over a finite field of square order, the notion of a SCRIM polynomial is defined in a similar fashion. For a polynomial

$$f(x) = \sum_{i=0}^{r} f_i x^i \in \mathbb{F}_{q^2}[x],$$

define its conjugate by

$$\overline{f}(x) = \sum_{i=0}^{r} f_i^q x^i.$$

The conjugate-reciprocal polynomial of $f(x)$ is $f^\dagger(x) = \overline{f^*}(x)$. A monic irreducible polynomial $f(x) \in \mathbb{F}_{q^2}[x]$ is called *SCRIM* if $f^\dagger(x) = f(x)$. The irreducible factor of $x^n - 1$ over $\mathbb{F}_{q^2}$ induced by a q^2-cyclotomic coset $\mathrm{Cl}_{q^2,n}(a)$ is

$$f_a(x) = \prod_{i \in \mathrm{Cl}_{q^2,n}(a)} (x - \zeta^i).$$

Its conjugate-reciprocal polynomial $f_a^\dagger(x)$ is induced by the coset $\mathrm{Cl}_{q^2,n}(-qa)$. Therefore, $f_a(x)$ is SCRIM if and only if

$$\mathrm{Cl}_{q^2,n}(a) = \mathrm{Cl}_{q^2,n}(-qa).$$

Equivalently, there exists a non-negative integer j such that $aq^{2j} \equiv -qa \pmod{n}$. Under the reduction modulo $\frac{n}{\gcd(n,a)}$, this is equivalent to

$$q^{2j} \equiv -q \pmod{\frac{n}{\gcd(n,a)}}.$$

For an odd prime p with $\gcd(p,q) = 1$, let γ be the unique positive integer such that $p^\gamma \parallel (q^{\mathrm{ord}_p(q)} - 1)$. For a positive integer s, let

$$\Delta_{p,q}(s) := \sum_{j=1}^{s} \frac{\varphi(p^j)}{\mathrm{ord}_{p^j}(q)},$$

where φ denotes Euler's phi function. The quantity $\Delta_{p,q}(s)$ has the concrete interpretation of counting the nonzero q-cyclotomic cosets in $\mathbb{Z}_{p^s}$, equivalently, the nontrivial monic irreducible factors of $x^{p^s} - 1$ over $\mathbb{F}_q$ (see Proposition 4.1 and [9, Section 4]). The following piecewise form of $\Delta_{p,q}(s)$ reflects the transition at the critical exponent γ: For $j \le \gamma$, the orders $\mathrm{ord}_{p^j}(q)$ remain constant, whereas for $j > \gamma$, they acquire an additional factor of $p^{j-\gamma}$, and this changes the corresponding cyclotomic coset's contributions. By Lemma 2.2 and the standard lifting property of multiplicative orders, this can be written explicitly as

$$\Delta_{p,q}(s) = \begin{cases} \dfrac{p^s - 1}{\mathrm{ord}_p(q)}, & \text{if } 1 \le s \le \gamma, \\ \dfrac{p^\gamma - 1}{\mathrm{ord}_p(q)} + \dfrac{(s-\gamma)p^{\gamma-1}(p-1)}{\mathrm{ord}_p(q)}, & \text{if } s > \gamma. \end{cases} \tag{4.1}$$

For each positive integer n, let $N_q(n)$ denote the number of monic irreducible factors of $x^n - 1$ over $\mathbb{F}_q$. The enumeration formula of $N_q(n)$ is presented in the following subsections.

4.1. Numbers of monic irreducible factors

With the notation introduced above, the standard divisor sum formula for the number of irreducible factors immediately gives the following convenient expression. The quantity $\Delta_{p,q}(s)$ will also be used repeatedly in the subsequent enumeration of irreducible, SRIM, and SCRIM factors, as well as in the resulting formulas for self-orthogonal cyclic codes.

Proposition 4.1. *Let q be a prime power and let p be an odd prime such that* $\gcd(p,q) = 1$. *Then,*

$$N_q(p^s) = 1 + \Delta_{p,q}(s).$$

Proof. We note that the number of monic irreducible factors of $x^n - 1$ over $\mathbb{F}_q$ is

$$N_q(p^s) = \sum_{d \mid p^s} \frac{\varphi(d)}{\mathrm{ord}_d(q)} = 1 + \sum_{j=1}^{s} \frac{\varphi(p^j)}{\mathrm{ord}_{p^j}(q)} = 1 + \Delta_{p,q}(s).$$

This proves the result. □

Example 4.2. *Let $q = 3$ and $p = 5$. Then,* $\mathrm{ord}_5(3) = 4$. *Since $3^4 - 1 = 80$ and $5^1 \parallel 80$, we have $\gamma = 1$, which implies that*

$$\Delta_{5,3}(s) = \frac{5^\gamma - 1}{\mathrm{ord}_5(3)} + \frac{(s-\gamma)5^{\gamma-1}(5-1)}{\mathrm{ord}_5(3)} = \frac{5-1}{4} + (s-1)\frac{4}{4} = s,$$

and

$$N_3(5^s) = 1 + \Delta_{5,3}(s) = s + 1$$

for all $s \geq 1$.

Remark 4.3. *We note that the case* $p = 2$ *requires separate treatment. Indeed, if* q *is odd, then the behavior of* $\mathrm{ord}_{2^s}(q)$ *depends on the 2-adic valuations of both* $q - 1$ *and* $q^2 - 1$. *More precisely, for* $s \geq 1$,

$$\mathrm{ord}_{2^s}(q) = \begin{cases} 1, & \text{if } 1 \leq s \leq \nu_2(q-1), \\ 2, & \text{if } \nu_2(q-1) < s \leq \nu_2(q^2-1), \\ 2^{s-\nu_2(q^2-1)+1}, & \text{if } s > \nu_2(q^2-1). \end{cases}$$

Consequently, the number of monic irreducible factors of $x^{2^s} - 1$ *over* $\mathbb{F}_q$ *is*

$$N_q(2^s) = \sum_{j=0}^{s} \frac{\varphi(2^j)}{\mathrm{ord}_{2^j}(q)},$$

where $\mathrm{ord}_1(q) = 1$. *However, unlike the odd-prime case, a closed formula for* $N_q(2^s)$ *is naturally piecewise according to* $\nu_2(q-1)$ *and* $\nu_2(q^2-1)$.

The separation conditions considered in Section 3 can be strengthened to obtain an important enumerative consequence. Under the hypotheses below, the relevant prime power orbit sizes are pairwise coprime, so that the divisor sum for the number of irreducible factors separates multiplicatively.

Theorem 4.4. *Let* q *be a prime power, and let* p_1 *and* p_2 *be the distinct odd primes such that* $\gcd(p_1 p_2, q) = 1$. *If* $\gcd(\mathrm{ord}_{p_1}(q), \mathrm{ord}_{p_2}(q)) = 1$, $p_1 \nmid \mathrm{ord}_{p_2}(q)$, *and* $p_2 \nmid \mathrm{ord}_{p_1}(q)$, *then,*

$$N_q(p_1^{s_1} p_2^{s_2}) = (1 + \Delta_{p_1,q}(s_1))(1 + \Delta_{p_2,q}(s_2)).$$

Proof. First, we note that each divisor of $p_1^{s_1} p_2^{s_2}$ has the form $p_1^{e_1} p_2^{e_2}$ for some $0 \leq e_1 \leq s_1$ and $0 \leq e_2 \leq s_2$. Set

$$d_1 = \mathrm{ord}_{p_1}(q) \text{ and } d_2 = \mathrm{ord}_{p_2}(q)$$

and let γ_t be the positive integer such that $p_t^{\gamma_t} \parallel (q^{d_t} - 1)$ for all $t = 1, 2$.

If $e_1 = 0$ or $e_2 = 0$, then one of $\mathrm{ord}_{p_1^{e_1}}(q)$ and $\mathrm{ord}_{p_2^{e_2}}(q)$ is equal to $\mathrm{ord}_1(q) = 1$. Hence, we have

$$\gcd(\mathrm{ord}_{p_1^{e_1}}(q), \mathrm{ord}_{p_2^{e_2}}(q)) = 1.$$

Assume that $e_1 \geq 1$ and $e_2 \geq 1$. Then,

$$\mathrm{ord}_{p_1^{e_1}}(q) = d_1 p_1^{\max\{e_1 - \gamma_1, 0\}} \text{ and } \mathrm{ord}_{p_2^{e_2}}(q) = d_2 p_2^{\max\{e_2 - \gamma_2, 0\}}$$

by Theorem 2.1. Since $d_t = \mathrm{ord}_{p_t}(q)$ divides $p_t - 1$ for $t = 1, 2$, we have $p_1 \nmid d_1$ and $p_2 \nmid d_2$. Together with the assumptions $\gcd(d_1, d_2) = 1$, $p_1 \nmid d_2$, and $p_2 \nmid d_1$, it follows that

$$\gcd(\mathrm{ord}_{p_1^{e_1}}(q), \mathrm{ord}_{p_2^{e_2}}(q)) = 1.$$

Consequently,

$$\operatorname{ord}_{p_1^{e_1}p_2^{e_2}}(q) = \operatorname{lcm}(\operatorname{ord}_{p_1^{e_1}}(q), \operatorname{ord}_{p_2^{e_2}}(q)) = \operatorname{ord}_{p_1^{e_1}}(q)\operatorname{ord}_{p_2^{e_2}}(q)$$

for all $0 \le e_1 \le s_1$ and $0 \le e_2 \le s_2$.

By the Chinese remainder theorem, we have

$$\mathbb{Z}_{p_1^{s_1}p_2^{s_2}} \cong \mathbb{Z}_{p_1^{s_1}} \times \mathbb{Z}_{p_2^{s_2}},$$

and multiplication by q corresponds to the diagonal action on the right-hand side. Since the sizes of the corresponding component q-cyclotomic cosets are coprime by the argument above, each pair of component q-cyclotomic cosets corresponds to exactly one q-cyclotomic coset modulo $p_1^{s_1}p_2^{s_2}$. Hence, the number of q-cyclotomic cosets, and, equivalently, the number of monic irreducible factors, separates multiplicatively.

Therefore,

$$\begin{aligned} N_q(p_1^{s_1}p_2^{s_2}) &= \sum_{e_1=0}^{s_1}\sum_{e_2=0}^{s_2}\frac{\varphi(p_1^{e_1}p_2^{e_2})}{\operatorname{ord}_{p_1^{e_1}p_2^{e_2}}(q)} \\ &= \sum_{e_1=0}^{s_1}\sum_{e_2=0}^{s_2}\frac{\varphi(p_1^{e_1})}{\operatorname{ord}_{p_1^{e_1}}(q)}\cdot\frac{\varphi(p_2^{e_2})}{\operatorname{ord}_{p_2^{e_2}}(q)} \\ &= \left(\sum_{e_1=0}^{s_1}\frac{\varphi(p_1^{e_1})}{\operatorname{ord}_{p_1^{e_1}}(q)}\right)\left(\sum_{e_2=0}^{s_2}\frac{\varphi(p_2^{e_2})}{\operatorname{ord}_{p_2^{e_2}}(q)}\right) \\ &= \Big(1+\Delta_{p_1,q}(s_1)\Big)\Big(1+\Delta_{p_2,q}(s_2)\Big) \end{aligned}$$

as desired. □

Illustrative examples are given as follows.

Example 4.5. *Let $q = 3$, $p_1 = 13$, and $p_2 = 11$. Then $\operatorname{ord}_{13}(3) = 3$ and $\operatorname{ord}_{11}(3) = 5$. Thus, $\gcd(\operatorname{ord}_{13}(3), \operatorname{ord}_{11}(3)) = \gcd(3,5) = 1, 13 \nmid \operatorname{ord}_{11}(3) = 5$, and $11 \nmid \operatorname{ord}_{13}(3) = 3$. Hence, the separation hypotheses in Theorem 4.4 are satisfied.*

For $p_1 = 13$, we have $3^3 - 1 = 26$ and $13^1 \parallel 26$. Hence, $\gamma_1 = 1$ and

$$\Delta_{13,3}(s_1) = \frac{13-1}{3} + (s_1 - 1)\frac{13-1}{3} = 4s_1.$$

For $p_2 = 11$, we have $3^5 - 1 = 242 = 2 \cdot 11^2$. Hence, $11^2 \parallel (3^5 - 1)$ which implies that $\gamma_2 = 2$. It follows that

$$\begin{aligned} \Delta_{11,3}(s_2) &= \begin{cases} \dfrac{11^{s_2}-1}{5}, & \text{if } 1 \le s_2 \le 2, \\ \dfrac{11^2-1}{5} + \dfrac{(s_2-2)11(11-1)}{5}, & \text{if } s_2 > 2, \end{cases} \\ &= \begin{cases} 2, & \text{if } s_2 = 1, \\ 24, & \text{if } s_2 = 2, \\ 24 + 22(s_2 - 2), & \text{if } s_2 > 2. \end{cases} \end{aligned}$$

By Theorem 4.4, we obtain

$$N_3(13^{s_1}11^{s_2}) = (1+\Delta_{13,3}(s_1))(1+\Delta_{11,3}(s_2))$$
$$= (4s_1+1)\begin{cases}3, & \text{if } s_2 = 1,\\ 25, & \text{if } s_2 = 2,\\ 25+22(s_2-2), & \text{if } s_2 > 2.\end{cases}$$

Example 4.6. *Let* $q = 11$, $p_1 = 13$, *and* $p_2 = 43$. *Then,* $\mathrm{ord}_{13}(11) = 12$ *and* $\mathrm{ord}_{43}(11) = 7$. *Thus,* $\gcd(\mathrm{ord}_{13}(11), \mathrm{ord}_{43}(11)) = \gcd(12,7) = 1$, $13 \nmid \mathrm{ord}_{43}(11) = 7$, *and* $43 \nmid \mathrm{ord}_{13}(11) = 12$. *Hence, the separation hypotheses in Theorem 4.4 are satisfied.*

For $p_1 = 13$, *we have* $13 \parallel (11^{12}-1)$, *so* $\gamma_1 = 1$. *By* (4.1), *it follows that*

$$\Delta_{13,11}(s_1) = \begin{cases}\dfrac{13^{s_1}-1}{12}, & \text{if } s_1 = 1,\\ \dfrac{13-1}{12} + \dfrac{(s_1-1)(13-1)}{12}, & \text{if } s_1 > 1,\end{cases}$$
$$= \begin{cases}1, & \text{if } s_1 = 1,\\ s_1, & \text{if } s_1 > 1.\end{cases}$$

For $p_2 = 43$, *we have* $43 \parallel (11^7-1)$, *so* $\gamma_2 = 1$. *Again by* (4.1), *we obtain*

$$\Delta_{43,11}(s_2) = \begin{cases}\dfrac{43^{s_2}-1}{7}, & \text{if } s_2 = 1,\\ \dfrac{43-1}{7} + \dfrac{(s_2-1)(43-1)}{7}, & \text{if } s_2 > 1,\end{cases}$$
$$= \begin{cases}6, & \text{if } s_2 = 1,\\ 6s_2, & \text{if } s_2 > 1.\end{cases}$$

By Theorem 4.4, we obtain

$$N_{11}(13^{s_1}43^{s_2}) = (1+\Delta_{13,11}(s_1))(1+\Delta_{43,11}(s_2))$$
$$= \begin{cases}14, & \text{if } s_1 = 1 \text{ and } s_2 = 1,\\ 12s_2+2, & \text{if } s_1 = 1 \text{ and } s_2 > 1,\\ 7(s_1+1), & \text{if } s_1 > 1 \text{ and } s_2 = 1,\\ (s_1+1)(6s_2+1), & \text{if } s_1 > 1 \text{ and } s_2 > 1.\end{cases}$$

We now extend the preceding results to the case

$$n = \prod_{t=1}^{\lambda} p_t^{s_t},$$

where $p_1, p_2, \ldots, p_\lambda$ are distinct odd primes such that $\gcd(n,q) = 1$. Before proceeding to the formula, we indicate the main idea. The number of monic irreducible factors of $x^n - 1$ over $\mathbb{F}_q$ is given by

$$N_q(n) = \sum_{d|n} \frac{\varphi(d)}{\mathrm{ord}_d(q)}.$$

For each $t \in \{1, 2, \ldots, \lambda\}$, let $d_t = \mathrm{ord}_{p_t}(q)$ and let γ_t be a positive integer such that $p_t^{\gamma_t} \parallel (q^{d_t} - 1)$. By Theorem 2.1, for every $1 \le e_t \le s_t$, we have

$$\mathrm{ord}_{p_t^{e_t}}(q) = d_t p_t^{\max\{e_t - \gamma_t, 0\}},$$

while $\mathrm{ord}_1(q) = 1$ when $e_t = 0$.

Suppose that $\gcd(d_u, d_v) = 1$ and $p_u \nmid d_v$ for all $u \neq v$. Since $d_t \mid (p_t - 1)$, we also have $p_t \nmid d_t$ for every t. Hence, for distinct values of u, v and all relevant exponents e_u, e_v, we have

$$\gcd(\mathrm{ord}_{p_u^{e_u}}(q), \mathrm{ord}_{p_v^{e_v}}(q)) = 1,$$

where the case $e_u = 0$ or $e_v = 0$ follows from $\mathrm{ord}_1(q) = 1$. Thus, for every divisor

$$d = \prod_{t=1}^{\lambda} p_t^{e_t}$$

of n, the corresponding prime power orders are pairwise coprime. Therefore, we have

$$\mathrm{ord}_d(q) = \mathrm{lcm}\left(\mathrm{ord}_{p_1^{e_1}}(q), \ldots, \mathrm{ord}_{p_\lambda^{e_\lambda}}(q)\right) = \prod_{t=1}^{\lambda} \mathrm{ord}_{p_t^{e_t}}(q).$$

This is the order separation property underlying the product formula in Theorem 4.7. Since Euler's phi function is also multiplicative on relatively prime factors, the divisor sum separates into a product of sums. Extending the idea in the proof of Theorem 4.4, we obtain the following result.

Theorem 4.7. *Let q be a prime power and let*

$$n = \prod_{t=1}^{\lambda} p_t^{s_t},$$

where $p_1, p_2, \ldots, p_\lambda$ are distinct odd primes; $s_1, s_2, \ldots, s_\lambda$ are positive integers; and $\gcd(n, q) = 1$. *If* $\gcd(\mathrm{ord}_{p_u}(q), \mathrm{ord}_{p_v}(q)) = 1$, *and $p_u \nmid \mathrm{ord}_{p_v}(q)$ for all $u \neq v$, then the number of monic irreducible factors of $x^n - 1$ over $\mathbb{F}_q$ is*

$$N_q(n) = \prod_{t=1}^{\lambda} (1 + \Delta_{p_t,q}(s_t)).$$

4.2. SRIM factors of $x^n - 1$

The preceding results lead naturally to the study of self-reciprocal irreducible monic factors of $x^n - 1$ over finite fields. Let $\mathrm{SRIM}_q(n)$ denote the number of self-reciprocal irreducible monic factors of $x^n - 1$ over $\mathbb{F}_q$. We first present results on SRIM factors of $x^n - 1$ over $\mathbb{F}_q$, with emphasis on the extremal cases where all irreducible factors are SRIM and where $x - 1$ is the unique SRIM factor.

Lemma 4.8. *([7]) Let q be a prime power and let p be an odd prime such that* $\gcd(p, q) = 1$. *Let s be a positive integer. Then the following statements hold:*

(1) All monic irreducible factors of $x^{p^s} - 1$ over $\mathbb{F}_q$ are SRIM if and only if $\mathrm{ord}_p(q)$ *is even.*

(2) The polynomial $x-1$ is the unique SRIM factor of $x^{p^s}-1$ over $\mathbb{F}_q$ if and only if $\mathrm{ord}_p(q)$ is odd.

Proposition 4.9. *Let q be a prime power.*

(1) Let p be an odd prime such that $\gcd(p,q)=1$. Then, we have

$$\mathrm{SRIM}_q(p^s)=\begin{cases}1, & \text{if } \mathrm{ord}_p(q) \text{ is odd},\\ 1+\Delta_{p,q}(s), & \text{if } \mathrm{ord}_p(q) \text{ is even}.\end{cases}$$

(2) For $\lambda \geq 2$, let

$$n=\prod_{t=1}^{\lambda} p_t^{s_t},$$

where $p_1, p_2, \ldots, p_\lambda$ are distinct odd primes such that $\gcd(n,q)=1$. If $\mathrm{ord}_{p_t}(q)$ is odd for every $1 \leq t \leq \lambda$, then $x-1$ is the unique SRIM factor of x^n-1 over $\mathbb{F}_q$.

Proof. The case of prime power follows from Lemma 4.8 and Proposition 4.1. For the latter case, if $\mathrm{ord}_{p_t}(q)$ is odd for every prime divisor p_t of n, then no nontrivial q-cyclotomic coset is fixed under negation. Hence, $x-1$ is the unique SRIM factor of x^n-1 over $\mathbb{F}_q$. □

Proposition 4.10. *Let q be a prime power, and let p_1 and p_2 be distinct odd primes such that $\gcd(p_1p_2,q)=1$. Assume that $\gcd(\mathrm{ord}_{p_1}(q), \mathrm{ord}_{p_2}(q))=1$, $p_1 \nmid \mathrm{ord}_{p_2}(q)$, and $p_2 \nmid \mathrm{ord}_{p_1}(q)$. If at least one of $\mathrm{ord}_{p_1}(q)$ and $\mathrm{ord}_{p_2}(q)$ is odd, then,*

$$\mathrm{SRIM}_q(p_1^{s_1}p_2^{s_2})=\mathrm{SRIM}_q(p_1^{s_1})\cdot\mathrm{SRIM}_q(p_2^{s_2}).$$

In particular,

$$\mathrm{SRIM}_q(p_1^{s_1}p_2^{s_2})=\begin{cases}1, & \text{if } \mathrm{ord}_{p_1}(q) \text{ and } \mathrm{ord}_{p_2}(q) \text{ are odd},\\ 1+\Delta_{p_1,q}(s_1), & \text{if } \mathrm{ord}_{p_1}(q) \text{ is even and } \mathrm{ord}_{p_2}(q) \text{ is odd},\\ 1+\Delta_{p_2,q}(s_2), & \text{if } \mathrm{ord}_{p_1}(q) \text{ is odd and } \mathrm{ord}_{p_2}(q) \text{ is even}.\end{cases}$$

Proof. The separation hypotheses imply that the irreducible factor enumeration for $x^{p_1^{s_1}p_2^{s_2}}-1$ separates according to the two prime power components by Theorem 4.4. If $\mathrm{ord}_{p_t}(q)$ is odd, then $x-1$ is the unique SRIM factor of $x^{p_t^{s_t}}-1$. Hence, this component contributes no nontrivial self-reciprocal factor. If the other component has and even order, then all irreducible factors from that prime power component are SRIM. Therefore, the number of SRIM factors is the product of the corresponding one prime counts. □

Example 4.11. *Let $q=3$, $p_1=41$, and $p_2=13$. Then, $p_1p_2=41\cdot 13=533$, $\mathrm{ord}_{41}(3)=8$, and $\mathrm{ord}_{13}(3)=3$. Hence, $\gcd(\mathrm{ord}_{41}(3),\mathrm{ord}_{13}(3))=\gcd(8,3)=1$, $41 \nmid \mathrm{ord}_{13}(3)=3$, and $13 \nmid \mathrm{ord}_{41}(3)=8$. Moreover, $\mathrm{ord}_{41}(3)$ is even and $\mathrm{ord}_{13}(3)$ is odd. Thus, the hypotheses of Proposition 4.10 are satisfied.*

For $p_1=41$, we have $41 \parallel (3^{\mathrm{ord}_{41}(3)}-1)=3^8-1=6560$, which implies that $\gamma_1=1$. By (4.1), we have

$$\Delta_{41,3}(1)=\frac{\varphi(41)}{\mathrm{ord}_{41}(3)}=\frac{40}{8}=5.$$

Since $\mathrm{ord}_{13}(3)$ *is odd, Proposition 4.10 gives*

$$\mathrm{SRIM}_3(533) = \mathrm{SRIM}_3(41 \cdot 13) = 1 + \Delta_{41,3}(1) = 6.$$

Therefore, $x^{533} - 1$ *over* $\mathbb{F}_3$ *has exactly six SRIM factors. The corresponding* 3*-cyclotomic cosets modulo* 533 *are as follows:*

$$\begin{aligned}
\mathrm{Cl}_{3,533}(0) &= \{0\},\\
\mathrm{Cl}_{3,533}(13) &= \{13, 39, 117, 351, 520, 494, 416, 182\},\\
\mathrm{Cl}_{3,533}(26) &= \{26, 78, 234, 169, 507, 455, 299, 364\},\\
\mathrm{Cl}_{3,533}(52) &= \{52, 156, 468, 338, 481, 377, 65, 195\},\\
\mathrm{Cl}_{3,533}(91) &= \{91, 273, 286, 325, 442, 260, 247, 208\},\\
\mathrm{Cl}_{3,533}(104) &= \{104, 312, 403, 143, 429, 221, 130, 390\}.
\end{aligned}$$

These 3*-cyclotomic cosets induce the six SRIM factors of* $x^{533} - 1$ *over* $\mathbb{F}_3$*. Since* $\mathbb{Z}_{533}$ *is quite large, we do not list the other* 3*-cyclotomic cosets explicitly, although they can be computed readily.*

In general, the number of SRIM factors of $x^n - 1$ over $\mathbb{F}_q$ does not satisfy a multiplicative formula with respect to the prime power decomposition of n. However, under suitable parity conditions on the relevant multiplicative orders, some simplified formulas can be derived. These observations are summarized in the following propositions.

Proposition 4.12. *Let* q *be a prime power, and let* p_1 *and* p_2 *be distinct odd primes such that* $\gcd(p_1 p_2, q) = 1$*. If* $\mathrm{ord}_{p_1}(q)$ *and* $\mathrm{ord}_{p_2}(q)$ *are even, and* $\nu_2(\mathrm{ord}_{p_1}(q)) \neq \nu_2(\mathrm{ord}_{p_2}(q))$*, then,*

$$\mathrm{SRIM}_q(p_1^{s_1} p_2^{s_2}) = 1 + \Delta_{p_1,q}(s_1) + \Delta_{p_2,q}(s_2).$$

Proof. By Theorem 2.1, we have

$$\mathrm{ord}_{p_t^{e_t}}(q) = \mathrm{ord}_{p_t}(q) p_t^{\max\{e_t - \gamma_t, 0\}}$$

for all $t = 1, 2$ and $1 \leq e_t \leq s_t$. Since p_t is odd, we have

$$\nu_2(\mathrm{ord}_{p_t^{e_t}}(q)) = \nu_2(\mathrm{ord}_{p_t}(q))$$

for all $t = 1, 2$ and $1 \leq e_t \leq s_t$.

We show that no mixed divisor $p_1^{e_1} p_2^{e_2}$, with $e_1, e_2 \geq 1$, contributes an SRIM factor. Such a factor is SRIM if and only if there exists $j \geq 0$ such that $q^j \equiv -1 \pmod{p_1^{e_1} p_2^{e_2}}$. Equivalently,

$$j \equiv \frac{\mathrm{ord}_{p_1^{e_1}}(q)}{2} \pmod{\mathrm{ord}_{p_1^{e_1}}(q)} \quad \text{and} \quad j \equiv \frac{\mathrm{ord}_{p_2^{e_2}}(q)}{2} \pmod{\mathrm{ord}_{p_2^{e_2}}(q)}.$$

By the Chinese remainder theorem, this system is solvable if and only if

$$\nu_2(\mathrm{ord}_{p_1^{e_1}}(q)) = \nu_2(\mathrm{ord}_{p_2^{e_2}}(q)).$$

Since p_1 and p_2 are odd, we have

$$\nu_2(\mathrm{ord}_{p_1^{e_1}}(q)) = \nu_2(\mathrm{ord}_{p_1}(q)) \quad \text{and} \quad \nu_2(\mathrm{ord}_{p_2^{e_2}}(q)) = \nu_2(\mathrm{ord}_{p_2}(q))$$

by Theorem 2.1. These valuations are distinct by hypothesis. Hence, no mixed divisor contributes an SRIM factor.

Since both $\mathrm{ord}_{p_1}(q)$ and $\mathrm{ord}_{p_2}(q)$ are even, Lemma 4.8 implies that all irreducible factors arising from the prime power divisors $p_1^{e_1}$ and $p_2^{e_2}$ are SRIM. Therefore, the SRIM factors are precisely $x-1$ together with the nontrivial prime power contributions. Hence, we have

$$\mathrm{SRIM}_q(p_1^{s_1}p_2^{s_2}) = 1 + \Delta_{p_1,q}(s_1) + \Delta_{p_2,q}(s_2)$$

as desired. □

Example 4.13. *Let $q = 3$, $p_1 = 37$, and $p_2 = 41$. Then, $p_1p_2 = 37 \cdot 41 = 1517$, $\mathrm{ord}_{37}(3) = 18$, and $\mathrm{ord}_{41}(3) = 8$. Thus, both orders are even and*

$$\nu_2(\mathrm{ord}_{37}(3)) = \nu_2(18) = 1 \neq 3 = \nu_2(8) = \nu_2(\mathrm{ord}_{41}(3)).$$

Hence, the hypotheses of Proposition 4.12 are satisfied. Since $37 \parallel (3^{18}-1)$ and $41 \parallel (3^8-1) = 6560$, we have $\gamma_1 = \gamma_2 = 1$. Therefore, by (4.1), it follows that

$$\Delta_{37,3}(1) = \frac{\varphi(37)}{\mathrm{ord}_{37}(3)} = \frac{36}{18} = 2$$

and

$$\Delta_{41,3}(1) = \frac{\varphi(41)}{\mathrm{ord}_{41}(3)} = \frac{40}{8} = 5.$$

By Proposition 4.12, we obtain

$$\mathrm{SRIM}_3(1517) = \mathrm{SRIM}_3(37 \cdot 41) = 1 + \Delta_{37,3}(1) + \Delta_{41,3}(1) = 1 + 2 + 5 = 8.$$

Therefore, $x^{1517}-1$ over $\mathbb{F}_3$ has exactly eight SRIM factors. Their corresponding 3-cyclotomic cosets modulo 1517 are as follows:

$$\begin{aligned}
\mathrm{Cl}_{3,1517}(0) &= \{0\},\\
\mathrm{Cl}_{3,1517}(37) &= \{37, 111, 333, 999, 1480, 1406, 1184, 518\},\\
\mathrm{Cl}_{3,1517}(41) &= \{41, 123, 369, 1107, 287, 861, 1066, 164, 492, 1476\},\\
\mathrm{Cl}_{3,1517}(74) &= \{74, 222, 666, 481, 1443, 1295, 851, 1036\},\\
\mathrm{Cl}_{3,1517}(82) &= \{82, 246, 738, 697, 574, 205, 615, 328, 984, 1435\},\\
\mathrm{Cl}_{3,1517}(148) &= \{148, 444, 1332, 962, 1369, 1073, 185, 555\},\\
\mathrm{Cl}_{3,1517}(259) &= \{259, 777, 814, 925, 1258, 740, 703, 592\},\\
\mathrm{Cl}_{3,1517}(296) &= \{296, 888, 1147, 407, 1221, 629, 370, 1110\}.
\end{aligned}$$

These 3-cyclotomic cosets induce the eight SRIM factors of $x^{1517}-1$ over $\mathbb{F}_3$. Since $\mathbb{Z}_{1517}$ is quite large, we omit the remaining 3-cyclotomic cosets, although they can be determined explicitly.

Proposition 4.14. *Let q be a prime power, and let p_1 and p_2 be distinct odd primes such that $\gcd(p_1p_2, q) = 1$. Assume that $\mathrm{ord}_{p_1}(q)$ and $\mathrm{ord}_{p_2}(q)$ are even, and*

$$a = \nu_2(\mathrm{ord}_{p_1}(q)) = \nu_2(\mathrm{ord}_{p_2}(q)).$$

If

$$\gcd\left(\frac{\operatorname{ord}_{p_1^{s_1}}(q)}{2^{\nu_2(\operatorname{ord}_{p_1^{s_1}}(q))}}, \frac{\operatorname{ord}_{p_2^{s_2}}(q)}{2^{\nu_2(\operatorname{ord}_{p_2^{s_2}}(q))}}\right) = 1,$$

then we have

$$\mathrm{SRIM}_q(p_1^{s_1}p_2^{s_2}) = 1 + \Delta_{p_1,q}(s_1) + \Delta_{p_2,q}(s_2) + 2^a\Delta_{p_1,q}(s_1)\Delta_{p_2,q}(s_2).$$

Proof. As in Proposition 4.12, all prime power contributions are SRIM and their total contribution is

$$\Delta_{p_1,q}(s_1) + \Delta_{p_2,q}(s_2),$$

together with the factor $x - 1$.

For a mixed divisor $p_1^{e_1}p_2^{e_2}$, the SRIM condition is equivalent to the simultaneous solvability of

$$q^j \equiv -1 \pmod{p_1^{e_1}} \quad \text{and} \quad q^j \equiv -1 \pmod{p_2^{e_2}}.$$

By the Chinese remainder theorem, this is equivalent to

$$\nu_2(\operatorname{ord}_{p_1^{e_1}}(q)) = \nu_2(\operatorname{ord}_{p_2^{e_2}}(q)).$$

By Theorem 2.1, these 2-adic valuations are equal to

$$\nu_2(\operatorname{ord}_{p_1}(q)) \text{ and } \nu_2(\operatorname{ord}_{p_2}(q)),$$

respectively. Hence, by the hypothesis, every mixed irreducible factor is SRIM.

It remains to count the mixed factors. For each mixed divisor $p_1^{e_1}p_2^{e_2}$, the number of irreducible factors contributed is

$$\frac{\varphi(p_1^{e_1})\varphi(p_2^{e_2})}{\operatorname{ord}_{p_1^{e_1}p_2^{e_2}}(q)}.$$

Assume that

$$\nu_2(\operatorname{ord}_{p_1^{e_1}}(q)) = \nu_2(\operatorname{ord}_{p_2^{e_2}}(q)) = a.$$

Write $\operatorname{ord}_{p_1^{e_1}}(q) = 2^a u_1$, and $\operatorname{ord}_{p_2^{e_2}}(q) = 2^a u_2$, where u_1 and u_2 are odd. Since

$$\gcd\left(\frac{\operatorname{ord}_{p_1^{s_1}}(q)}{2^{\nu_2(\operatorname{ord}_{p_1^{s_1}}(q))}}, \frac{\operatorname{ord}_{p_2^{s_2}}(q)}{2^{\nu_2(\operatorname{ord}_{p_2^{s_2}}(q))}}\right) = 1$$

at the top-degree orders, then $\gcd(u_1, u_2) = 1$. It follows that

$$\operatorname{lcm}(\operatorname{ord}_{p_1^{e_1}}(q), \operatorname{ord}_{p_2^{e_2}}(q)) = \operatorname{lcm}(2^a u_1, 2^a u_2) = 2^a u_1 u_2 = \frac{\operatorname{ord}_{p_1^{e_1}}(q)\operatorname{ord}_{p_2^{e_2}}(q)}{2^a}.$$

Therefore, the mixed contribution is

$$2^a\left(\sum_{e_1=1}^{s_1}\frac{\varphi(p_1^{e_1})}{\operatorname{ord}_{p_1^{e_1}}(q)}\right)\left(\sum_{e_2=1}^{s_2}\frac{\varphi(p_2^{e_2})}{\operatorname{ord}_{p_2^{e_2}}(q)}\right) = 2^a\Delta_{p_1,q}(s_1)\Delta_{p_2,q}(s_2).$$

Adding the contributions from $x - 1$, the pure prime power parts, and the mixed part gives the desired formula. □

Example 4.15. *Let $q = 3$, $p_1 = 41$, and $p_2 = 241$. Then, $p_1p_2 = 41 \cdot 241 = 9881$, $\mathrm{ord}_{41}(3) = 8$, and $\mathrm{ord}_{241}(3) = 120$. Hence, both orders are even and*

$$\nu_2(\mathrm{ord}_{41}(3)) = \nu_2(8) = 3 \quad \textit{and} \quad \nu_2(\mathrm{ord}_{241}(3)) = \nu_2(120) = 3.$$

Thus,

$$a = \nu_2(\mathrm{ord}_{41}(3)) = \nu_2(\mathrm{ord}_{241}(3)) = 3.$$

Moreover, $41 \parallel (3^8 - 1) = 6560$ and $241 \parallel (3^{120} - 1)$, which implies that $\gamma_1 = \gamma_2 = 1$. By (4.1), we have

$$\Delta_{41,3}(1) = \frac{\varphi(41)}{\mathrm{ord}_{41}(3)} = \frac{40}{8} = 5$$

and

$$\Delta_{241,3}(1) = \frac{\varphi(241)}{\mathrm{ord}_{241}(3)} = \frac{240}{120} = 2.$$

In this case, we have $s_1 = s_2 = 1$, and it follows that

$$\frac{\mathrm{ord}_{41}(3)}{2^{\nu_2(\mathrm{ord}_{41}(3))}} = \frac{8}{8} = 1$$

and

$$\frac{\mathrm{ord}_{241}(3)}{2^{\nu_2(\mathrm{ord}_{241}(3))}} = \frac{120}{8} = 15.$$

Therefore, we have

$$\gcd\left(\frac{\mathrm{ord}_{41}(3)}{2^{\nu_2(\mathrm{ord}_{41}(3))}}, \frac{\mathrm{ord}_{241}(3)}{2^{\nu_2(\mathrm{ord}_{241}(3))}}\right) = \gcd(1, 15) = 1.$$

Hence, the hypotheses of Proposition 4.14 are satisfied. By Proposition 4.14, we have

$$\begin{aligned}\mathrm{SRIM}_3(9881) &= \mathrm{SRIM}_3(41 \cdot 241)\\ &= 1 + \Delta_{41,3}(1) + \Delta_{241,3}(1) + 2^3\Delta_{41,3}(1)\Delta_{241,3}(1)\\ &= 1 + 5 + 2 + 8 \cdot 5 \cdot 2 = 88.\end{aligned}$$

Therefore, $x^{9881} - 1$ over $\mathbb{F}_3$ has exactly 88 SRIM factors. Since $\mathbb{Z}_{9881}$ is fairly large, we do not display all the corresponding 3-cyclotomic cosets explicitly, although they can be determined without difficulty.

4.3. SCRIM factors of $x^n - 1$

In this subsection, we next turn to the Hermitian analog over finite fields of square order. Let $\mathrm{SCRIM}_{q^2}(n)$ denote the number of self-conjugate-reciprocal irreducible monic factors of $x^n - 1$ over $\mathbb{F}_{q^2}$. We then establish the corresponding results on SCRIM factors of $x^n - 1$ over $\mathbb{F}_{q^2}$, again focusing on the extremal cases where all irreducible factors are SCRIM and where $x - 1$ is the unique SCRIM factor.

Proposition 4.16. *([10, Theorem 2.13]) Let q be a prime power and let λ be a positive integer. Let*

$$n = \prod_{t=1}^{\lambda} p_t^{s_t},$$

where $p_1, p_2, \ldots, p_\lambda$ are distinct odd primes such that $\gcd(n, q) = 1$. Then, the following statements hold:

(1) The polynomial $x-1$ is the unique SCRIM factor of x^n-1 over $\mathbb{F}_{q^2}$ if and only if, for every $t \in \{1,2,\ldots,\lambda\}$, we have

$$\mathrm{ord}_{p_t}(q^2) \text{ is even or } \mathrm{ord}_{p_t}(q) \text{ is odd.}$$

(2) All monic irreducible factors of x^n-1 over $\mathbb{F}_{q^2}$ are SCRIM if and only if, for every $t \in \{1,2,\ldots,\lambda\}$, we have

$$\mathrm{ord}_{p_t}(q^2) \text{ is odd and } \mathrm{ord}_{p_t}(q) \text{ is even.}$$

Proposition 4.17. *Let q be a prime power and let p be an odd prime such that $\gcd(p,q)=1$. Then,*

$$\mathrm{SCRIM}_{q^2}(p^s) = \begin{cases} 1, & \text{if } \mathrm{ord}_p(q^2) \text{ is even or } \mathrm{ord}_p(q) \text{ is odd,} \\ 1+\Delta_{p,q^2}(s), & \text{if } \mathrm{ord}_p(q^2) \text{ is odd and } \mathrm{ord}_p(q) \text{ is even.} \end{cases}$$

Proof. The results follow directly from Proposition 4.16. In the case where all monic irreducible factors of $x^{p^s}-1$ over $\mathbb{F}_{q^2}$ are SCRIM, we have

$$\mathrm{SCRIM}_{q^2}(p^s) = N_{q^2}(p^s) = 1+\Delta_{p,q^2}(s),$$

by an argument similar to the proof of Proposition 4.1, with q^2 in place of q. □

When all irreducible factors are SCRIM, the number of SCRIM factors is simply the total number of monic irreducible factors. Under the same separation condition used in the finite prime enumeration, this total number admits the following product formula.

Proposition 4.18. *Let q be a prime power and let λ be a positive integer. Let*

$$n = \prod_{t=1}^{\lambda} p_t^{s_t},$$

where $p_1, p_2 \ldots, p_\lambda$ are distinct odd primes and $\gcd(n,q)=1$. For each $t \in \{1,2,\ldots,\lambda\}$, let $p_t^{\gamma'_t} \parallel ((q^2)^{\mathrm{ord}_{p_t}(q^2)}-1)$. Assume that for every $t \in \{1,2,\ldots,\lambda\}$, $\mathrm{ord}_{p_t}(q^2)$ is odd and $\mathrm{ord}_{p_t}(q)$ is even. Assume also that the following separation conditions hold: $\gcd(\mathrm{ord}_{p_u}(q^2), \mathrm{ord}_{p_v}(q^2)) = 1$ for all $u \neq v$ and, for every $u \in \{1,2,\ldots,\lambda\}$, $s_u = \gamma'_u$ or $p_u \nmid \mathrm{ord}_{p_v}(q^2)$ for all $v \neq u$. Then,

$$\mathrm{SCRIM}_{q^2}(n) = \prod_{t=1}^{\lambda} (1+\Delta_{p_t,q^2}(s_t)).$$

Proof. By Proposition 4.16, the assumptions $\mathrm{ord}_{p_t}(q^2)$ is odd and $\mathrm{ord}_{p_t}(q)$ is even for all t imply that all monic irreducible factors of x^n-1 over $\mathbb{F}_{q^2}$ are SCRIM. The additional separation conditions ensure, by the same order separation argument used before Theorem 4.7, that

$$N_{q^2}(n) = \prod_{t=1}^{\lambda} (1+\Delta_{p_t,q^2}(s_t)).$$

Since all monic irreducible factors are SCRIM, the desired formula follows. □

5. Applications to self-orthogonal cyclic codes

In this section, we focus on self-orthogonal cyclic codes. Some preliminary results on such codes were discussed in [4, 15]. Our main point here is that the recursive factorization results established above provide an effective tool for the enumeration of such codes. Indeed, they reduce the factorization of $x^n - 1$ at higher degrees to the corresponding factorization at suitable critical degrees, thereby giving a structured description of the generator polynomials involved. The enumeration is then presented in terms of the distribution of SRIM and SCRIM factors of $x^n - 1$ over the underlying finite fields.

5.1. Cyclic codes and their Euclidean and Hermitian duals

A linear code of length n over $\mathbb{F}_q$ is an $\mathbb{F}_q$-subspace of the $\mathbb{F}_q$-vector space $\mathbb{F}_q^n$. If C has a dimension k and the minimum Hamming distance

$$d = \min\{\mathrm{wt}(\boldsymbol{c}) : \boldsymbol{c} \in C \setminus \{\boldsymbol{0}\}\},$$

then, C is called an $[n, k, d]_q$ linear code, where $\mathrm{wt}(\boldsymbol{c})$ is the number of non-zero positions in $\boldsymbol{c}$. For $\boldsymbol{u} = (u_0, u_1, \ldots, u_{n-1}), \boldsymbol{v} = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_q^n$, the *Euclidean inner product* is defined by

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle_{\mathrm{E}} = \sum_{i=0}^{n-1} u_i v_i.$$

The *Euclidean dual of a linear code* C of length n over $\mathbb{F}_q$ is

$$C^{\perp_{\mathrm{E}}} = \{\boldsymbol{u} \in \mathbb{F}_q^n : \langle \boldsymbol{u}, \boldsymbol{v} \rangle_{\mathrm{E}} = 0 \text{ for all } \boldsymbol{v} \in C\}.$$

The code C is called *Euclidean self-orthogonal* if $C \subseteq C^{\perp_{\mathrm{E}}}$.

Over $\mathbb{F}_{q^2}$, the *Hermitian inner product* is defined by

$$\langle \boldsymbol{u}, \boldsymbol{v} \rangle_{\mathrm{H}} = \sum_{i=0}^{n-1} u_i v_i^q$$

for all $\boldsymbol{u} = (u_0, u_1, \ldots, u_{n-1})$ and $\boldsymbol{v} = (v_0, v_1, \ldots, v_{n-1}) \in \mathbb{F}_{q^2}^n$. The *Hermitian dual of a linear code* C over $\mathbb{F}_{q^2}$ is

$$C^{\perp_{\mathrm{H}}} = \{\boldsymbol{u} \in \mathbb{F}_{q^2}^n : \langle \boldsymbol{u}, \boldsymbol{v} \rangle_{\mathrm{H}} = 0 \text{ for all } \boldsymbol{v} \in C\}.$$

The code C is called *Hermitian self-orthogonal* if $C \subseteq C^{\perp_{\mathrm{H}}}$.

A linear code C of length n over $\mathbb{F}_q$ is called *cyclic* if every cyclic shift of a codeword in C is again a codeword in C. Cyclic codes of length n over $\mathbb{F}_q$ can be identified with ideals of the principal ideal ring $\mathbb{F}_q[x]/\langle x^n - 1\rangle$. Moreover, every cyclic code is generated by a unique monic divisor $g(x)$ of $x^n - 1$, which is called the *generator polynomial* of C [1]. If C is a cyclic code of length n over $\mathbb{F}_q$ with the generator polynomial $g(x)$, then, $\dim(C) = n - \deg(g(x))$. The polynomial $h(x) = (x^n - 1)/g(x)$ is called the *parity-check polynomial* of C.

The following standard facts describe the Euclidean and Hermitian duals of cyclic codes in terms of parity-check polynomial.

Proposition 5.1. *([2]) Let C be a cyclic code of length n over $\mathbb{F}_q$ with the generator polynomial $g(x)$ and let $h(x) = (x^n - 1)/g(x)$. Then, the Euclidean dual $C^{\perp_E}$ is the cyclic code generated by $h^*(x)$.*

Proposition 5.2. *([5]) Let C be a cyclic code of length n over $\mathbb{F}_{q^2}$ with generator polynomial $g(x)$ and let $h(x) = (x^n - 1)/g(x)$. Then, the Hermitian dual $C^{\perp_H}$ is the cyclic code generated by $h^\dagger(x)$.*

Consequently, the self-orthogonality conditions for cyclic codes can be expressed purely in terms of the divisibility of generator and parity-check polynomials.

Theorem 5.3. *Let C be a cyclic code of length n with generator polynomial $g(x)$ and let $h(x) = (x^n - 1)/g(x)$. Then, the following statements hold:*

(1) Over $\mathbb{F}_q$, the code C is Euclidean self-orthogonal if and only if $h^*(x) \mid g(x)$.
(2) Over $\mathbb{F}_{q^2}$, the code C is Hermitian self-orthogonal if and only if $h^\dagger(x) \mid g(x)$.

5.2. Enumeration of Euclidean self-orthogonal cyclic codes

Let $\mathbb{F}_q$ be a finite field of characteristic ρ and let $n = m\rho^u$, where $u \geq 0$ and $\gcd(m, \rho) = 1$. We emphasize that over a finite field of characteristic ρ, we have $(a - b)^{\rho^u} = a^{\rho^u} - b^{\rho^u}$. Consequently, we have

$$x^{m\rho^u} - 1 = (x^m - 1)^{\rho^u}.$$

This identity plays a key role later in the enumeration developed in this section, especially in Theorem 5.4 and its subsequent corollaries.

According to the discussion above, the repeated-root factorization of $x^n - 1$ is completely determined by the simple root factorization of $x^m - 1$. In particular, the recursive factorization results obtained earlier for $x^m - 1$ can be used directly in the repeated-root setting.

Suppose that the factorization of $x^m - 1$ over $\mathbb{F}_q$ is

$$x^m - 1 = \prod_{i=1}^{r} f_i(x) \prod_{j=1}^{t} h_j(x) h_j^*(x),$$

where $f_1(x), \ldots, f_r(x)$ are SRIM factors and $(h_j(x), h_j^*(x))$ are reciprocal pairs of irreducible factors for all $j = 1, 2, \ldots, t$. Then,

$$x^{m\rho^u} - 1 = \prod_{i=1}^{r} f_i(x)^{\rho^u} \prod_{j=1}^{t} h_j(x)^{\rho^u} h_j^*(x)^{\rho^u}. \tag{5.1}$$

Hence, every cyclic code of length $m\rho^u$ over $\mathbb{F}_q$ has aa generator polynomial of the form

$$g(x) = \prod_{i=1}^{r} f_i(x)^{\alpha_i} \prod_{j=1}^{t} h_j(x)^{\beta_j} h_j^*(x)^{\delta_j},$$

where $0 \leq \alpha_i, \beta_j, \delta_j \leq \rho^u$.

The following elementary counting result serves as the bridge between the polynomial factorization and the enumeration of Euclidean self-orthogonal cyclic codes. Its significance here lies in allowing the SRIM and reciprocal pair counts obtained in the preceding sections to be converted directly into code enumeration formulas.

Theorem 5.4. *Let $\mathbb{F}_q$ be a finite field of characteristic ρ and let $n = m\rho^u$ with $u \geq 0$ and* $\gcd(m, \rho) = 1$. *Assume the factorization in* (5.1). *Then the number of Euclidean self-orthogonal cyclic codes of length $m\rho^u$ over $\mathbb{F}_q$ is*

$$\left(\left\lfloor \frac{\rho^u}{2} \right\rfloor + 1\right)^r \left(\frac{(\rho^u + 1)(\rho^u + 2)}{2}\right)^t.$$

Proof. Let

$$g(x) = \prod_{i=1}^{r} f_i(x)^{\alpha_i} \prod_{j=1}^{t} h_j(x)^{\beta_j} h_j^*(x)^{\delta_j},$$

where $0 \leq \alpha_i, \beta_j, \delta_j \leq \rho^u$. Then,

$$h(x) = \frac{x^{m\rho^u} - 1}{g(x)} = \prod_{i=1}^{r} f_i(x)^{\rho^u - \alpha_i} \prod_{j=1}^{t} h_j(x)^{\rho^u - \beta_j} h_j^*(x)^{\rho^u - \delta_j}.$$

By Theorem 5.3 (1), the code $\langle g(x) \rangle$ is Euclidean self-orthogonal if and only if $h^*(x) \mid g(x)$. Since each $f_i(x)$ is self-reciprocal, this is equivalent to $\rho^u - \alpha_i \leq \alpha_i$ for all $i = 1, 2, \ldots, r$, and $\rho^u - \delta_j \leq \beta_j$ and $\rho^u - \beta_j \leq \delta_j$ for all $j = 1, 2, \ldots, t$. Thus,

$$\alpha_i \geq \left\lceil \frac{\rho^u}{2} \right\rceil,$$

so each SRIM factor contributes

$$\rho^u - \left\lceil \frac{\rho^u}{2} \right\rceil + 1 = \left\lfloor \frac{\rho^u}{2} \right\rfloor + 1$$

choices. For each reciprocal pair, the two inequalities are equivalent to

$$\beta_j + \delta_j \geq \rho^u.$$

Hence, the number of admissible pairs (β_j, δ_j) with $0 \leq \beta_j, \delta_j \leq \rho^u$ is

$$\frac{(\rho^u + 1)(\rho^u + 2)}{2}.$$

Multiplying over all SRIM factors and all reciprocal pairs, the result follows. □

With the terms introduced in Section 4, for a positive integer m such that $\gcd(\rho, m) = 1$, we have

$$r = \mathrm{SRIM}_q(m) \quad \text{and} \quad t = \frac{N_q(m) - \mathrm{SRIM}_q(m)}{2}. \tag{5.2}$$

By Theorem 5.4, the number of Euclidean self-orthogonal cyclic codes of length $m\rho^u$ over $\mathbb{F}_q$ is

$$\left(\left\lfloor \frac{\rho^u}{2} \right\rfloor + 1\right)^{\mathrm{SRIM}_q(m)} \left(\frac{(\rho^u + 1)(\rho^u + 2)}{2}\right)^{\frac{N_q(m) - \mathrm{SRIM}_q(m)}{2}}.$$

In the case where $u = 0$, this result reduces to the simple root case and we have

$$\left(\left\lfloor \frac{1}{2} \right\rfloor + 1\right)^r = 1 \text{ and } \left(\frac{(1 + 1)(1 + 2)}{2}\right)^t = 3^t. \tag{5.3}$$

Therefore, by Theorem 5.4, the number of Euclidean self-orthogonal cyclic codes of length n over $\mathbb{F}_q$ with $\gcd(n, q) = 1$ is 3^t.

The following example illustrates a coding theoretic consequence of the enumeration formulas above for a product of two distinct odd prime powers. It directly uses the separation framework developed in the preceding sections.

Example 5.5. *Consider cyclic codes over $\mathbb{F}_{11}$ of length $n = 13^{s_1}43^{s_2}$, where $s_1, s_2 \geq 1$. As shown in Example 4.6, the separation hypotheses are satisfied and*

$$N_{11}(13^{s_1}43^{s_2}) = (s_1 + 1)(6s_2 + 1).$$

Moreover, since $\mathrm{ord}_{13}(11) = 12$ *is even and* $\mathrm{ord}_{43}(11) = 7$ *is odd, Proposition 4.10 gives*

$$\mathrm{SRIM}_{11}(13^{s_1}43^{s_2}) = s_1 + 1.$$

Hence, the number of reciprocal pairs is

$$\frac{N_{11}(13^{s_1}43^{s_2}) - \mathrm{SRIM}_{11}(13^{s_1}43^{s_2})}{2} = 3s_2(s_1 + 1).$$

Consequently, by Theorem 5.4 with $u = 0$, the number of Euclidean self-orthogonal cyclic codes of length $13^{s_1}43^{s_2}$ over $\mathbb{F}_{11}$ is $3^{3s_2(s_1+1)}$.

We now record repeated-root versions of the preceding Euclidean enumeration formulas by combining the SRIM counts for the simple root part with Theorem 5.4.

Corollary 5.6. *Let $\mathbb{F}_q$ be a finite field of characteristic ρ and let p be an odd prime such that*

$$\gcd(p, q) = 1.$$

Let $p^\gamma \parallel (q^{\mathrm{ord}_p(q)} - 1)$. Then, the number of Euclidean self-orthogonal cyclic codes of length $p^s\rho^u$ over $\mathbb{F}_q$ is

$$\begin{cases} \left(\left\lfloor \dfrac{\rho^u}{2} \right\rfloor + 1\right)^{1+\Delta_{p,q}(s)}, & \text{if } \mathrm{ord}_p(q) \text{ is even}, \\ \left(\left\lfloor \dfrac{\rho^u}{2} \right\rfloor + 1\right)\left(\dfrac{(\rho^u + 1)(\rho^u + 2)}{2}\right)^{\frac{\Delta_{p,q}(s)}{2}}, & \text{if } \mathrm{ord}_p(q) \text{ is odd}, \end{cases}$$

where $\Delta_{p,q}(s)$ is given in terms of s and γ in (4.1).

Proof. The proof can be given by applying Theorem 5.4 with $m = p^s$. If $\mathrm{ord}_p(q)$ is even, then all irreducible factors of $x^{p^s} - 1$ over $\mathbb{F}_q$ are SRIM. Hence, we have

$$\mathrm{SRIM}_q(p^s) = N_q(p^s) = 1 + \Delta_{p,q}(s)$$

which implies that $r = 1 + \Delta_{p,q}(s)$ and $t = 0$. If $\mathrm{ord}_p(q)$ is odd, then $x - 1$ is the unique SRIM factor of $x^{p^s} - 1$ over $\mathbb{F}_q$. Hence,

$$r = 1 \qquad \text{and} \qquad t = \frac{N_q(p^s) - 1}{2} = \frac{\Delta_{p,q}(s)}{2}.$$

Substituting these values into Theorem 5.4, the result follows. □

The following examples illustrate the recursive enumeration formulas for Euclidean self-orthogonal cyclic codes over finite fields.

Example 5.7. *Let $p = 13$ and $q = 3$. Then, $\mathrm{ord}_{13}(3) = 3$ is odd. The polynomial $x - 1$ is the unique SRIM factor of $x^{13^s} - 1$ over $\mathbb{F}_3$ for all $s \geq 1$ by Lemma 4.8.*

For $s = 1$, the factorization of $x^{13} - 1$ over $\mathbb{F}_3$ has the form

$$x^{13} - 1 = (x - 1)h_1(x)h_1^*(x)h_2(x)h_2^*(x),$$

where $h_1(x) = x^3 - x - 1$ and $h_2(x) = x^3 - x^2 - x - 1$. Thus, there are two reciprocal pairs, and hence there exist $3^2 = 9$ Euclidean self-orthogonal cyclic codes of length 13 over $\mathbb{F}_3$.

Since $13 \parallel (3^{\mathrm{ord}_{13}(3)} - 1)$, we have $\gamma = 1$. Therefore, $\Delta_{13,3}(s) = 4s$ for all $s \geq 1$. Hence, the number of Euclidean self-orthogonal cyclic codes of length 13^s over $\mathbb{F}_3$ is 3^{2s}. In particular, we have values shown in the Table 1.

Table 1. Number of Euclidean self-orthogonal cyclic codes of length 13^s over $\mathbb{F}_3$.

s	13^s	Number of Euclidean self-orthogonal cyclic codes
1	13	$3^2 = 9$
2	169	$3^4 = 81$
3	2197	$3^6 = 729$
4	28561	$3^8 = 6561$

Example 5.8. *Let $p = 7$ and $q = 11$. Then, $\mathrm{ord}_7(11) = 3$ is odd. By Lemma 4.8, $x - 1$ is the unique SRIM factor of $x^{7^s} - 1$ over $\mathbb{F}_{11}$.*

For $s = 1$, the factorization of $x^7 - 1$ over $\mathbb{F}_{11}$ is

$$x^7 - 1 = (x - 1)(x^3 - 4x^2 - 5x - 1)(x^3 + 5x^2 + 4x - 1).$$

Since

$$(x^3 - 4x^2 - 5x - 1)^* = x^3 + 5x^2 + 4x - 1,$$

there is exactly one reciprocal pair. Hence, there exist $3^1 = 3$ Euclidean self-orthogonal cyclic codes of length 7 over $\mathbb{F}_{11}$.

Since $7 \parallel (11^{\mathrm{ord}_7(11)} - 1) = 11^3 - 1 = 1330$, we have $\gamma = 1$. Therefore, $\Delta_{7,11}(s) = 2s$ for all $s \geq 1$. Hence, the number of Euclidean self-orthogonal cyclic codes of length 7^s over $\mathbb{F}_{11}$ is 3^s. In particular, we have the values shown in Table 2.

Table 2. Number of Euclidean self-orthogonal cyclic codes of length 7^s over $\mathbb{F}_{11}$.

s	7^s	Number of Euclidean self-orthogonal cyclic codes
1	7	3
2	49	9
3	343	27
4	2401	81

Corollary 5.9. *Let $\mathbb{F}_q$ be a finite field of characteristic ρ, and let p_1 and p_2 be distinct odd primes such that $\gcd(p_1p_2, q) = 1$. If s_1 and s_2 are positive integers and $u \geq 0$, then the following statements hold.*

(1) If both $\mathrm{ord}_{p_1}(q)$ *and* $\mathrm{ord}_{p_2}(q)$ *are odd, then the number of Euclidean self-orthogonal cyclic codes of length* $p_1^{s_1}p_2^{s_2}\rho^u$ *over* $\mathbb{F}_q$ *is*

$$\left(\left\lfloor \frac{\rho^u}{2} \right\rfloor + 1\right)\left(\frac{(\rho^u+1)(\rho^u+2)}{2}\right)^{\frac{N_q(p_1^{s_1}p_2^{s_2})-1}{2}}.$$

(2) If both $\mathrm{ord}_{p_1}(q)$ *and* $\mathrm{ord}_{p_2}(q)$ *are even and* $\nu_2(\mathrm{ord}_{p_1}(q)) \neq \nu_2(\mathrm{ord}_{p_2}(q))$*, then the number of Euclidean self-orthogonal cyclic codes of length* $p_1^{s_1}p_2^{s_2}\rho^u$ *over* $\mathbb{F}_q$ *is*

$$\left(\left\lfloor \frac{\rho^u}{2} \right\rfloor + 1\right)^{1+\Delta_{p_1,q}(s_1)+\Delta_{p_2,q}(s_2)}\left(\frac{(\rho^u+1)(\rho^u+2)}{2}\right)^{\frac{N_q(p_1^{s_1}p_2^{s_2})-1-\Delta_{p_1,q}(s_1)-\Delta_{p_2,q}(s_2)}{2}}.$$

Proof. The proof can be given via Theorem 5.4 by setting $m = p_1^{s_1}p_2^{s_2}$. In Case (1), Proposition 4.9 gives $\mathrm{SRIM}_q(p_1^{s_1}p_2^{s_2}) = 1$ which implies that $r = 1$ and

$$t = \frac{N_q(p_1^{s_1}p_2^{s_2}) - 1}{2}.$$

In Case (2), Proposition 4.12 gives

$$\mathrm{SRIM}_q(p_1^{s_1}p_2^{s_2}) = 1 + \Delta_{p_1,q}(s_1) + \Delta_{p_2,q}(s_2).$$

Hence, we have

$$r = 1 + \Delta_{p_1,q}(s_1) + \Delta_{p_2,q}(s_2) \quad \text{and} \quad t = \frac{N_q(p_1^{s_1}p_2^{s_2}) - 1 - \Delta_{p_1,q}(s_1) - \Delta_{p_2,q}(s_2)}{2}.$$

Substituting these values into Theorem 5.4, the result follows. □

The following example complements Corollary 5.9 by providing an explicit code construction. It also illustrates the recursive factorization for a product of two prime powers in Corollary 3.7, where both prime power exponents are strictly greater than their corresponding critical exponents.

Example 5.10. *Consider cyclic codes of length* $n = 5^2 7^2 = 1225$ *over* $\mathbb{F}_3$*. Here,* $s_1 = s_2 = 2$*. We have* $\mathrm{ord}_5(3) = 4$ *and* $\mathrm{ord}_7(3) = 6$*. Since* $5 \parallel (3^4 - 1)$ *and* $7 \parallel (3^6 - 1)$*, we have*

$$\gamma_1 = \gamma_2 = 1.$$

Hence, $s_1 > \gamma_1$ *and* $s_2 > \gamma_2$*. Since* $5 \nmid 6$ *and* $7 \nmid 4$*, the hypotheses of Corollary 3.7 are satisfied. Thus, the critical degree is* $n_0 = 5 \cdot 7 = 35$*.*

Over $\mathbb{F}_3$*, we have*

$$x^{35} - 1 = (x-1)f_1(x)f_2(x)g_1(x)g_2(x),$$

where

$$f_1(x) = x^4 + x^3 + x^2 + x + 1,$$
$$f_2(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1,$$
$$g_1(x) = x^{12} + x^{10} - x^8 + x^7 + x^5 - x^4 + x^3 - x^2 - x + 1,$$

and

$$g_2(x) = x^{12} - x^{11} - x^{10} + x^9 - x^8 + x^7 + x^5 - x^4 + x^2 + 1.$$

The roots of $f_1(x)$, $f_2(x)$, $g_1(x)$, *and* $g_2(x)$ *have multiplicative orders* 5, 7, 35, *and* 35, *respectively. Hence,*

$$\mathcal{F}_\varnothing = \{x-1\}, \mathcal{F}_1 = \{f_1\}, \mathcal{F}_2 = \{f_2\}, \text{ and } \mathcal{F}_{12} = \{g_1, g_2\}.$$

By Corollary 3.7, we have

$$\begin{aligned} x^{1225} - 1 &= \prod_{f\in\mathcal{F}_\varnothing} f(x) \prod_{f\in\mathcal{F}_1}\prod_{j_1=0}^{1} f(x^{5^{j_1}}) \prod_{f\in\mathcal{F}_2}\prod_{j_2=0}^{1} f(x^{7^{j_2}}) \prod_{f\in\mathcal{F}_{12}}\prod_{j_1=0}^{1}\prod_{j_2=0}^{1} f(x^{5^{j_1}7^{j_2}}) \\ &= (x-1)f_1(x)f_1(x^5)f_2(x)f_2(x^7)\prod_{i=1}^{2} g_i(x)g_i(x^5)g_i(x^7)g_i(x^{35}). \end{aligned}$$

We next relate this factorization to Corollary 5.9. Since $\nu_2(\mathrm{ord}_5(3)) = 2$ *and* $\nu_2(\mathrm{ord}_7(3)) = 1$, *the hypotheses of Corollary 5.9 (2) are satisfied. From the factorization above, we have*

$$N_3(1225) = 1 + 2 + 2 + 8 = 13.$$

Moreover, $\Delta_{5,3}(2) = 2$ *and* $\Delta_{7,3}(2) = 2$. *Hence, by Proposition 4.12, we have*

$$\mathrm{SRIM}_3(1225) = 1 + \Delta_{5,3}(2) + \Delta_{7,3}(2) = 5.$$

Thus, the number of reciprocal pairs is

$$\frac{N_3(1225) - \mathrm{SRIM}_3(1225)}{2} = \frac{13-5}{2} = 4.$$

Since the length 1225 *is coprime to the characteristic* 3, *we have* $u = 0$ *in Corollary 5.9. Hence, the number of Euclidean self-orthogonal cyclic codes of length* 1225 *over* $\mathbb{F}_3$ *is*

$$3^4 = 81.$$

We now construct one of these codes explicitly. Since

$$g_1^*(x) = g_2(x),$$

let $C = \langle G(x)\rangle$ *be a cyclic code of length* 1225 , *where*

$$G(x) = (x-1)f_1(x)f_1(x^5)f_2(x)f_2(x^7)g_1(x)g_2(x)g_1(x^5)g_1(x^7)g_1(x^{35}).$$

Its parity-check polynomial is

$$H(x) = \frac{x^{1225}-1}{G(x)} = g_2(x^5)g_2(x^7)g_2(x^{35}).$$

Hence,

$$H^*(x) = g_1(x^5)g_1(x^7)g_1(x^{35})$$

and $H^*(x) \mid G(x)$*. Consequently, C is Euclidean self-orthogonal by Theorem 5.3. Since*

$$\deg(H(x)) = 12 \cdot 5 + 12 \cdot 7 + 12 \cdot 35 = 60 + 84 + 420 = 564,$$

we have $\dim(C) = 564$*. A computation using the Magma computational algebra system [16] gives*

$$d(C) = 12.$$

Therefore, the constructed Euclidean self-orthogonal cyclic code has the parameters

$$[1225, 564, 12]_3.$$

A direct comparison with a best known ternary code of the same length and dimension was not available from the public databases consulted. For reference, the Griesmer bound (see, for example, [7]) gives

$$d \leq 444$$

for a ternary linear code of length 1225 *and dimension* 564*, since*

$$\sum_{i=0}^{563} \left\lceil \frac{444}{3^i} \right\rceil = 1225 \quad \textit{and} \quad \sum_{i=0}^{563} \left\lceil \frac{445}{3^i} \right\rceil = 1227 > 1225.$$

Thus, the purpose of this example is to demonstrate an explicit and verifiable application of the two-dimensional recursive factorization, rather than to claim the optimality of the resulting code.

5.3. Enumeration of Hermitian self-orthogonal cyclic codes

We next consider Hermitian self-orthogonal cyclic codes of length

$$n = m\rho^u$$

over $\mathbb{F}_{q^2}$, where $\rho = \mathrm{char}(\mathbb{F}_{q^2})$, $u \geq 0$, and $\gcd(m, \rho) = 1$. Assume that

$$x^m - 1 = \prod_{i=1}^{r} f_i(x) \prod_{j=1}^{t} h_j(x) h_j^{\dagger}(x),$$

where $f_1(x), f_2(x), \ldots, f_r(x)$ are SCRIM factors and $(h_j(x), h_j^{\dagger}(x))$ is a conjugate-reciprocal pair of irreducible factors for every $j = 1, 2, \ldots, t$. We note that, over a finite field of characteristic ρ, we have $(a - b)^{\rho^u} = a^{\rho^u} - b^{\rho^u}$. Consequently

$$x^{m\rho^u} - 1 = (x^m - 1)^{\rho^u} = \prod_{i=1}^{r} f_i(x)^{\rho^u} \prod_{j=1}^{t} h_j(x)^{\rho^u} h_j^{\dagger}(x)^{\rho^u}. \tag{5.4}$$

Hence, every cyclic code of length $m\rho^u$ over $\mathbb{F}_{q^2}$ has a generator polynomial of the form

$$g(x) = \prod_{i=1}^{r} f_i(x)^{\alpha_i} \prod_{j=1}^{t} h_j(x)^{\beta_j} h_j^{\dagger}(x)^{\delta_j},$$

where $0 \leq \alpha_i, \beta_j, \delta_j \leq \rho^u$.

The corresponding Hermitian enumeration follows from the same counting principle, with SCRIM factors and conjugate-reciprocal pairs replacing SRIM factors and reciprocal pairs.

Theorem 5.11. *Let $\mathbb{F}_{q^2}$ be a finite field of characteristic ρ and let $n = m\rho^u$ with $u \geq 0$ and $\gcd(m, \rho) = 1$. Assume the factorization of $x^{m\rho^u} - 1$ is as in* (5.4)*. Then, the number of Hermitian self-orthogonal cyclic codes of length $m\rho^u$ over $\mathbb{F}_{q^2}$ is*

$$\left(\left\lfloor \frac{\rho^u}{2} \right\rfloor + 1\right)^r \left(\frac{(\rho^u + 1)(\rho^u + 2)}{2}\right)^t.$$

Proof. The proof can be given using arguments similar to those in the proof of Theorem 5.4 for the Euclidean case and Theorem 5.3 (2). □

Given the notations given in Section 4, we have

$$r = \mathrm{SCRIM}_{q^2}(m) \quad \text{and} \quad t = \frac{N_{q^2}(m) - \mathrm{SCRIM}_{q^2}(m)}{2}$$

and the number of Hermitian self-orthogonal cyclic codes of length $m\rho^u$ over $\mathbb{F}_{q^2}$ is

$$\left(\left\lfloor \frac{\rho^u}{2} \right\rfloor + 1\right)^{\mathrm{SCRIM}_{q^2}(m)} \left(\frac{(\rho^u + 1)(\rho^u + 2)}{2}\right)^{\frac{N_{q^2}(m) - \mathrm{SCRIM}_{q^2}(m)}{2}}.$$

For $u = 0$, this reduces to the simple root case, and hence the number of Hermitian self-orthogonal cyclic codes of length m over $\mathbb{F}_{q^2}$ is 3^t.

From Theorem 5.11 and Proposition 4.17, the following corollaries can be deduced directly and the proofs are omitted.

Corollary 5.12. *Let $\mathbb{F}_{q^2}$ be a finite field of characteristic ρ, and let p be an odd prime such that $\gcd(p, q) = 1$. Let s be a positive integer and let $u \geq 0$. Then, the number of Hermitian self-orthogonal cyclic codes of length $p^s\rho^u$ over $\mathbb{F}_{q^2}$ is*

$$\begin{cases} \left(\left\lfloor \frac{\rho^u}{2} \right\rfloor + 1\right)\left(\frac{(\rho^u + 1)(\rho^u + 2)}{2}\right)^{\frac{\Delta_{p,q^2}(s)}{2}}, & \text{if } \mathrm{ord}_p(q^2) \text{ is even or } \mathrm{ord}_p(q) \text{ is odd,} \\ \left(\left\lfloor \frac{\rho^u}{2} \right\rfloor + 1\right)^{1+\Delta_{p,q^2}(s)}, & \text{if } \mathrm{ord}_p(q^2) \text{ is odd and } \mathrm{ord}_p(q) \text{ is even.} \end{cases}$$

Corollary 5.13. *Let $\mathbb{F}_{q^2}$ be a finite field of characteristic ρ, and let p_1 and p_2 be distinct odd primes such that $\gcd(p_1p_2, q) = 1$. Let s_1, s_2 be positive integers and let $u \geq 0$. Let $m = p_1^{s_1}p_2^{s_2}$. Then, the following statements hold:*

(1) If, for each $t \in \{1, 2\}$, $\mathrm{ord}_{p_t}(q^2)$ is even or $\mathrm{ord}_{p_t}(q)$ is odd, then, the number of Hermitian self-orthogonal cyclic codes of length $m\rho^u$ over $\mathbb{F}_{q^2}$ is

$$\left(\left\lfloor \frac{\rho^u}{2} \right\rfloor + 1\right)\left(\frac{(\rho^u + 1)(\rho^u + 2)}{2}\right)^{\frac{N_{q^2}(m)-1}{2}}.$$

(2) If, for each $t \in \{1, 2\}$, $\mathrm{ord}_{p_t}(q^2)$ is odd and $\mathrm{ord}_{p_t}(q)$ is even, $\gcd(\mathrm{ord}_{p_1}(q^2), \mathrm{ord}_{p_2}(q^2)) = 1$, $p_1 \nmid \mathrm{ord}_{p_2}(q^2)$, and $p_2 \nmid \mathrm{ord}_{p_1}(q^2)$, then, the number of Hermitian self-orthogonal cyclic codes of length $m\rho^u$ over $\mathbb{F}_{q^2}$ is

$$\left(\left\lfloor \frac{\rho^u}{2} \right\rfloor + 1\right)^{\left(1+\Delta_{p_1,q^2}(s_1)\right)\left(1+\Delta_{p_2,q^2}(s_2)\right)}.$$

Example 5.14. *Let $p = 5$ and $q = 3$, and let a be a primitive element of $\mathbb{F}_{3^2}$. Then* $\mathrm{ord}_5(3) = 4$ *and* $\mathrm{ord}_5(3^2) = \mathrm{ord}_5(9) = 2$. *Thus,* $\mathrm{ord}_5(3^2)$ *is even. Hence, by Proposition 4.17, the polynomial $x - 1$ is the unique SCRIM factor of $x^{5^s} - 1$ over $\mathbb{F}_{3^2}$ for all $s \geq 1$.*

For $s = 1$, we have

$$x^5 - 1 = (x - 1)(x^2 + ax + 1)(x^2 + a^3x + 1)$$

over $\mathbb{F}_{3^2}$, where $x - 1$ is the unique SCRIM factor and $(x^2 + ax + 1, x^2 + a^3x + 1)$ forms a conjugate-reciprocal pair. Therefore, by Corollary 5.12, the number of Hermitian self-orthogonal cyclic codes of length 5 over $\mathbb{F}_{3^2}$ is 3. Since $5^1 \parallel ((3^2)^{\mathrm{ord}_5(3^2)} - 1) = 9^2 - 1 = 80$, we have $\gamma = 1$. Hence,

$$\Delta_{5,3^2}(s) = 2s.$$

By Corollary 5.12, the number of Hermitian self-orthogonal cyclic codes of length 5^s over $\mathbb{F}_{3^2}$ is

$$3^{\frac{\Delta_{5,3^2}(s)}{2}} = 3^s.$$

In particular, we have Table 3.

Table 3. Number of Hermitian self-orthogonal cyclic codes of length 5^s over $\mathbb{F}_{3^2}$.

s	5^s	Number of Hermitian self-orthogonal cyclic codes
1	5	3
2	25	9
3	125	27
4	625	81

6. Conclusions

In this paper, we presented an alternative view of the recursive factorization patterns of $x^n - 1$ over finite fields, special factor enumerations, and applications to self-orthogonal cyclic codes. Beginning with the prime power case $n = p^s$, we showed that suitable irreducible factors induced by q-cyclotomic cosets can be obtained recursively through power substitutions. This recursive description was then extended to products of two prime powers and, more generally, to certain finite products of distinct prime powers under suitable separation conditions on the relevant multiplicative orders. These recursive factorizations provide explicit templates for the factorization of $x^n - 1$ at higher degrees once the factorization at a suitable critical degree is known. In particular, they reduce the problem of factoring $x^n - 1$ for large values of n to the determination of certain base factors and their subsequent power substitutions.

We also derived formulas for the number of monic irreducible factors of $x^n - 1$ in the prime power, a product of two prime powers, and a finite product of prime powers. By introducing the contribution function $\Delta_{p,q}(s)$, the enumeration was expressed in a compact form. Under the separation hypothesis, the total number of irreducible factors was shown to decompose multiplicatively according to the prime power components of n.

As applications, we used these enumerative results to describe SRIM and SCRIM factors in several important cases. In particular, we obtained clean characterizations for the extremal situations where

$x-1$ is the unique SRIM or SCRIM factor and where all monic irreducible factors are SRIM or SCRIM. These results were then applied to enumerate Euclidean and Hermitian self-orthogonal cyclic codes.

From this perspective, the main contribution of the present work is not a new general algorithm for factoring $x^n - 1$ over finite fields, but an explicit recursive and enumerative framework that is particularly well suited to applications in algebraic coding theory.

Several directions remain open for future work. One natural problem is to weaken the separation condition on the multiplicative orders while still retaining a usable recursive factorization pattern. In the present paper, the recursive power substitution method depends crucially on the fact that the order contributions from the different prime power components remain separated so that the corresponding q-cyclotomic cosets decompose into uniform blocks. If this condition is relaxed, then extra divisibility interactions among distinct prime power components may enter the multiplicative order, and the clean block structure of the cosets may break down. As a result, the recursive factorization may no longer be expressible in the same simple form, and a more refined analysis of mixed order interactions would be required. Another interesting direction is to obtain sharper formulas for the number of SRIM factors in mixed divisor cases, where the interaction between different prime power components becomes more subtle. It would also be worthwhile to investigate further applications of self-orthogonal cyclic codes, especially to the construction and study of quantum codes; see, for example, [17, 18].

Author contributions

A. Boripan: conceptualization, methodology, formal analysis, investigation, resources, writing–original draft, visualization, project administration, funding acquisition, software; S. Jitman: methodology, formal analysis, investigation, writing–review and editing, validation.

More specifically, A. Boripan initiated the main idea of the study; developed the case of prime case; prepared the enumeration of irreducible SRIM and SCRIM factors; organized the applications to self-orthogonal cyclic codes; and prepared the manuscript. S. Jitman developed and refined the recursive factorization results for the products of two prime powers and the finite products of distinct prime powers; verified the mathematical correctness of the results; provided corrections and revisions throughout the manuscript; and handled manuscript communication. All authors have read and agreed to the published version of the manuscript.

Use of Generative-AI tools declaration

The authors declare they used Artificial Intelligence (AI) tools for language editing of this article.

Acknowledgments

This research was supported by the National Research Council of Thailand (NRCT) under Grant Number N42A660938. The authors would like to thank the anonymous referees for their helpful comments.

Conflict of interest

The authors declare no conflicts of interest.

References

1. R. Lidl, H. Niederreiter, *Finite fields*, Cambridge University Press, 2008. https://doi.org/10.1017/CBO9780511525926
2. S. Ling, C. Xing, *Coding theory: a first course*, Cambridge University Press, 2004. https://doi.org/10.1017/CBO9780511755279
3. S. Prugsapitak, S. Jitman, Enumeration of self-dual cyclic codes of some specific lengths over finite fields, *Discrete Math. Algorithms Appl.*, **10** (2018), 1850031. https://doi.org/10.1142/S1793830918500313
4. K. Qian, S. Zhu, X. Kai, On cyclic self-orthogonal codes over $\mathbb{Z}_{2^m}$, *Finite Fields Appl.*, **33** (2015), 54–65. https://doi.org/10.1016/j.ffa.2014.11.005
5. E. Sangwisut, S. Jitman, S. Ling, P. Udomkavanich, Hulls of cyclic and negacyclic codes over finite fields, *Finite Fields Appl.*, **33** (2015), 232–257. https://doi.org/10.1016/j.ffa.2014.12.008
6. Y. Jia, S. Ling, C. Xing, On self-dual cyclic codes over finite fields, *IEEE Trans. Inf. Theory*, **57** (2011), 2243–2251. https://doi.org/10.1109/TIT.2010.2092415
7. W. C. Huffman, V. Pless, *Fundamentals of error-correcting codes*, Cambridge University Press, 2003. https://doi.org/10.1017/CBO9780511807077
8. I. F. Blake, X. H. Gao, R. C. Mullin, S. A. Vanstone, T. Yaghoobian, *Applications of finite fields*, Springer, 1993. https://doi.org/10.1007/978-1-4757-2226-0
9. B. Chen, S. Ling, G. Zhang, Enumeration formulas for self dual cyclic codes, *Finite Fields Appl.*, **42** (2016), 1–22. https://doi.org/10.1016/j.ffa.2016.06.007
10. A. Boripan, S. Jitman, P. Udomkavanich, Self-conjugate-reciprocal irreducible monic factors of $x^n - 1$ over finite fields and their applications, *Finite Fields Appl.*, **55** (2019), 78–96. https://doi.org/10.1016/j.ffa.2018.09.004
11. S. Jitman, Good integers and some applications in coding theory, *Cryptography Commun.*, **10** (2018), 685–704. https://doi.org/10.1007/s12095-017-0255-4
12. S. Jitman, S. Prugsapitak, M. Raka, Some generalizations of good integers and their applications in the study of self-dual negacyclic codes, *Adv. Math. Commun.*, **14** (2020), 35–51. https://doi.org/10.3934/amc.2020004
13. P. Moree, On the divisors of $a^k + b^k$, *Acta Arith.*, **80** (1997), 197–212. http://doi.org/10.4064/AA-80-3-197-212
14. M. B. Nathanson, *Elementary methods in number theory*, Springer, 2000. https://doi.org/10.1007/b98870
15. J. Zhang, X. Kai, P. Li, Self-orthogonal cyclic codes with good parameters, *Finite Fields Appl.*, **101** (2025), 102534. https://doi.org/10.1016/j.ffa.2024.102534

16. W. Bosma, J. Cannon, C. Playoust, The Magma algebra system I: the user language, *J. Symbolic Comput.*, **24** (1997), 235–265. https://doi.org/10.1006/jsco.1996.0125

17. E. Knill, R. Laflamme, Theory of quantum error-correcting codes, *Phys. Rev. A*, **55** (1997), 900–911. https://doi.org/10.1103/PhysRevA.55.900

18. A. Ashikhmin, E. Knill, Nonbinary quantum stabilizer codes, *IEEE Trans. Inf. Theory*, **47** (2001), 3065–3072. https://doi.org/10.1109/18.959288

AIMS Press