AIMS Mathematics, 9(9): 23468–23488.
DOI: 10.3934/math.20241141
Received: 19 June 2024
Revised: 25 July 2024
Accepted: 26 July 2024
Published: 05 August 2024

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

Research article

On the number of the irreducible factors of $x^n - 1$ over finite fields

Weitao Xie, Jiayu Zhang and Wei Cao*

School of Mathematics and Statistics, Minnan Normal University, Zhangzhou 363000, China

* **Correspondence:** Email: caow2286@mnnu.edu.cn.

Abstract: Let $\mathbb{F}_q$ be the finite field of q elements, and $\mathbb{F}_{q^n}$ its extension of degree n. A normal basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ is a basis of the form $\{\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}\}$. Some problems on normal bases can be finally reduced to the determination of the irreducible factors of the polynomial $x^n - 1$ in $\mathbb{F}_q$, while the latter is closely related to the cyclotomic polynomials. Denote by $\mathfrak{F}(x^n - 1)$ the set of all distinct monic irreducible factors of $x^n - 1$ in $\mathbb{F}_q$. The criteria for

$$|\mathfrak{F}(x^n - 1)| \leq 2$$

have been studied in the literature. In this paper, we provide the sufficient and necessary conditions for

$$|\mathfrak{F}(x^n - 1)| = s,$$

where s is a positive integer by using the properties of cyclotomic polynomials and results from the Diophantine equations. As an application, we obtain the sufficient and necessary conditions for

$$|\mathfrak{F}(x^n - 1)| = 3, 4, 5.$$

Keywords: finite fields; normal basis; irreducible factors; Diophantine equation; cyclotomic polynomial
Mathematics Subject Classification: 11D04, 11T06

1. Introduction

The study of Diophantine equations plays a very important role in number theory, and the integer solutions of Diophantine equations are widely used in cryptography and coding theory. Silverman [1] studied the parametric solution of equation

$$X^3 + Y^3 = A,$$

Li and Yuan [2] proved that the simultaneous Pell equations possess at most one positive integer solution under certain conditions.

A Diophantine equation of the form

$$a_1x_1 + a_2x_2 + \cdots + a_tx_t = s \tag{1.1}$$

is called a multivariate linear Diophantine equation, where $s, a_1, a_2, \cdots, a_t$ are nonzero integers and $t \geq 2$. It is well known that for any given nonzero integers a and b, there are two integers u and v such that

$$ua + vb = (a, b),$$

where (a, b) represents the greatest common divisor of a and b. Now we introduce some symbols associated with Eq (1.1) as follows:

$$(a_1, a_2) = d_2, (d_2, a_3) = d_3, \cdots, (d_{t-1}, a_t) = d_t.$$

That is, there exist integers $u_1, u_2, \cdots, u_t$ and $v_2, v_3, \cdots, v_{t-1}$ such that

$$\begin{cases} a_1u_1 + a_2u_2 = d_2, \\ d_2v_2 + a_3u_3 = d_3, \\ \quad\vdots \\ d_{t-1}v_{t-1} + a_tu_t = d_t. \end{cases} \tag{1.2}$$

Li [3] gave the structure of the general solution of the multivariate linear Diophantine equation.

Theorem 1.1. ([3]) *The multivariate linear Diophantine Eq* (1.1) *has solutions if and only if* $d_t|s$. *Furthermore, if* $d_t|s$ *and* $t \geq 4$, *then the general solutions of Diophantine Eq* (1.1) *are*

$$\begin{cases} x_1 = u_1(\delta \prod_{2\leq i\leq t-1} v_i + \sum_{4\leq j\leq t} \bar{a}_j \prod_{2\leq i\leq j-2} v_i s_{j-1} + \bar{a}_3 s_2) + \bar{a}_2 s_1, \\ x_2 = u_2(\delta \prod_{2\leq i\leq t-1} v_i + \sum_{4\leq j\leq t} \bar{a}_j \prod_{2\leq i\leq j-2} v_i s_{j-1} + \bar{a}_3 s_2) - a_1 d_2^{-1} s_1, \\ x_3 = u_3(\delta \prod_{3\leq i\leq t-1} v_i + \sum_{5\leq j\leq t} \bar{a}_j \prod_{3\leq i\leq j-2} v_i s_{j-1} + \bar{a}_4 s_3) - d_2 d_3^{-1} s_2, \\ \quad\vdots \\ x_{t-1} = u_{t-1}(\delta v_{t-1} + \bar{a}_t s_{t-1}) - d_{t-2} d_{t-1}^{-1} s_{t-2}, \\ x_t = u_t\delta - d_{t-1} d_t^{-1} s_{t-1}, \end{cases} \tag{1.3}$$

where $s_i (1 \leq i \leq t-1)$ *are arbitrary integers and* $\delta = sd_t^{-1}, \bar{a}_j = a_j d_j^{-1}$ *for* $2 \leq j \leq t$.

Let $\mathbb{F}_q$ be a finite field of q elements with characteristic p, and $\mathbb{F}_{q^n}$ be its extension of degree n, where p is a prime number and $n \geq 2$ is an integer. Zhu et al. [4] obtained an explicit formula for the number of solutions to the equation

$$f(x_1) + \cdots + f(x_n) = a$$

over $\mathbb{F}_q$. Zhao et al. [5] found an explicit formula for the number of solutions of the two-variable diagonal quartic equation

$$x_1^4 + x_2^4 = c$$

over $\mathbb{F}_q$.

A basis of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ of the form $\{\alpha, \alpha^q, \cdots, \alpha^{q^{n-1}}\}$ is called a *normal basis* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$, and α is called a *normal element* of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. An irreducible polynomial $f(x) \in \mathbb{F}_q[x]$ is called a *normal polynomial* if all the roots of $f(x)$ are normal elements of $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$. The *trace* of α is defined as

$$Tr(\alpha) = \alpha + \alpha^q + \cdots + \alpha^{q^{n-1}}$$

and the *trace* of $f(x)$ is defined to be the coefficient of x^{n-1}. Theorems 1.1 and 1.2 below give a simple criterion to check when an irreducible polynomial is a *normal polynomial*.

Theorem 1.2. ([6]) *Let $n = p^e$ with $e \geq 1$. Then an irreducible polynomial*

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{F}_q[x]$$

is a normal polynomial if and only if $a_1 \neq 0$.

Theorem 1.3. ([7]) *Let n be a prime different from p, and let q be a primitive root modulo n. Then an irreducible polynomial*

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{F}_q[x]$$

is a normal polynomial if and only if $a_1 \neq 0$.

In 2001, Chang([8]) et al. furthermore proved that the conditions in Theorems 1.1 and 1.2 are also necessary.

Theorem 1.4. ([8]) *If every irreducible polynomial*

$$f(x) = x^n + a_1 x^{n-1} + \cdots + a_n \in \mathbb{F}_q[x]$$

with $a_1 \neq 0$ is a normal polynomial, then n is either a power of p or a prime different from p, and q is a primitive root modulo n.

In 2018, Huang et al. [9] presented a unified proof of Theorems 1.1–1.3 by comparing the number of normal polynomials and that of irreducible polynomials over $\mathbb{F}_q$.

The factorization of $x^n - 1$ and its irreducible factors are closely related to the normal elements in $\mathbb{F}_{q^n}$ over $\mathbb{F}_q$ (see [10, Section 2]). Denote by $\mathfrak{F}(x^n - 1)$ the set of all distinct monic irreducible factors of $x^n - 1$ in a given finite field, $\Phi_r(x)$ a r-th cyclotomic polynomial, and $\varphi(\cdot)$ the Euler function. Write

$$n = mp^e,$$

where $e \geq 0$ is an integer, p is the characteristic of $\mathbb{F}_q$, and $p \nmid m$. Below are the known results for

$$|\mathfrak{F}(x^n - 1)| = 1, 2.$$

Theorem 1.5. ([11]) *The following statements are equivalent:*

(a) $|\mathfrak{F}(x^n - 1)| = 1$.

(b) $\mathfrak{F}(x^n - 1)=\{x - 1\}$.

(c) $n = p^e$.

Theorem 1.6. ([11]) *The following statements are equivalent:*

(a) $|\mathfrak{F}(x^n - 1)| = 2$.

(b) $\mathfrak{F}(x^n - 1)=\{x - 1, 1 + x + \cdots + x^{m-1}\}$.

(c) *m is a prime different from p, and q is a primitive root modulo m.*

We summarize the five theorems above into the theorem below:

Theorem 1.7. *The following statements are equivalent:*

(a) *Every irreducible polynomial of degree n over $\mathbb{F}_q$ with a nonzero trace is a normal polynomial.*

(b) $\mathfrak{F}(x^n - 1) \subseteq \{x - 1, 1 + x + \cdots + x^{n-1}\}$.

(c) (c1) $n = p^e$, *or*

(c2) n is a prime different from p, with q being a primitive root modulo n.

Cao [11] presented a new and unified proof of Theorem 1.6 and also extended Theorem 1.6. In this paper, we give the necessary and sufficient condition for the polynomial $x^n - 1$ to have s different irreducible factors for a given positive integer s.

2. Preliminaries

Lemma 2.1 indicates that factorization of $x^n - 1$ in finite fields is closely related to the cyclotomic polynomials.

Lemma 2.1. ([12]) *Let $\mathbb{F}_q$ be a finite field of characteristic p, and let n be a positive integer not divisible by p. Then*

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

Lemma 2.2. ([13]) *Let l be the order of a modulo m, $a^n \equiv 1$ (mod m), then $l \mid n$.*

Lemma 2.3. ([12]) *Let $\mathbb{F}_q$ be a finite field and n a positive integer with $(q, n) = 1$. Then the cyclotomic polynomial $\Phi_n(x)$ factors into $\frac{\varphi(n)}{d}$ distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of the same degree d, where d is the order of q modulo n.*

Lemma 2.4 is the well-known theorem about the existence of primitive roots.

Lemma 2.4. ([14]) *Let n be a positive integer. Then n possesses primitive roots if and only if n is of the form 2, 4, p^α, or $2p^\alpha$, where p is an odd prime and α is a positive integer.*

By Lemmas 2.3 and 2.4, we have the following lemma:

Lemma 2.5. *The cyclotomic polynomial $\Phi_n(x)$ is irreducible over $\mathbb{F}_q$ if and only if $n = 2, 4, p^\alpha, 2p^\alpha$, and q is a primitive root modulo n.*

We define $v_p(x)$ to be the greatest power in which a prime p divides x, that is, if $v_p(x) = \alpha$, then $p^\alpha | x$ but $p^{\alpha+1} \nmid x$. The following lemma is called the *lifting the exponent lemma* (*LTE*):

Lemma 2.6. ([15]) *Let x and y be (not necessarily positive) integers, n be a positive integer, and p be an odd prime such that $p|x - y$ and none of x and y is divisible by p. We have*

$$v_p(x^n - y^n) = v_p(x - y) + v_p(n).$$

Lemma 2.7. *Let p be an odd prime and g be a primitive root modulo p^2, with $(g, p) = 1$. Then g is a primitive root modulo $p^l (l \geq 1)$.*

Proof. We first prove that g is a primitive root modulo $p^l (l \geq 2)$ by induction on l. Let g be a primitive root modulo p^l. The order of g modulo p^{l+1} is d. We have

$$\varphi(p^l) \mid d, d \mid \varphi(p^{l+1}),$$

which shows that

$$d = p^{l-1}(p - 1)$$

or

$$d = p^l(p - 1).$$

We next prove that

$$d \neq p^{l-1}(p - 1).$$

According to Euler's theorem, we have

$$g^{p^{l-2}(p-1)} \equiv 1 \pmod{p^{l-1}},$$

there exists an integer k such that

$$g^{p^{l-2}(p-1)} = 1 + kp^{l-1},$$

since g is a primitive root modulo p^l, we have

$$g^{p^{l-2}(p-1)} \not\equiv 1 \pmod{p^l},\ p^l \nmid kp^{l-1},\ (k, p) = 1.$$

Obviously, for $l \geq 2$, we have

$$2l - 1 \geq l + 1$$

and

$$3(l - 1) \geq l + 1,$$

which shows that

$$\begin{aligned} g^{p^{l-1}(p-1)} &= (1 + kp^{l-1})^p \\ &= 1 + kp^l + k^2 \frac{p(p-1)}{2} p^{2(l-1)} + tp^{3(l-1)} + \cdots \\ &\equiv 1 + kp^l (mod p^{l+1}), \end{aligned}$$

where t is an integer and $(k, p) = 1$. It follows that

$$g^{p^{l-1}(p-1)} \equiv 1 + kp^l \not\equiv 1 \pmod{p^{l+1}}.$$

Therefore

$$d \neq p^{l-1}(p - 1),\ \ d = p^l(p - 1),$$

and g is a primitive root modulo p^{l+1}.

We next use the LTE to prove that g is a primitive root modulo p. The Euler's theorem shows that

$$g^{\varphi(p)} \equiv 1 (mod p),$$

since g is a primitive root modulo p^2, we have

$$v_p(g^{\varphi(p)} - 1) = 1.$$

Let h be the order of g modulo p, then $h|\varphi(p)$. Similarly, we can obtain

$$v_p(g^h - 1) = 1.$$

Let $x = g^h$, $y = 1$, then $(p, g^h) = 1$, $p|g^h - 1$. By the LTE, we have

$$v_p(g^{ph} - 1) = v_p(g^h - 1) + v_p(p) = 1 + 1 = 2,$$

which shows that

$$p^2|g^{ph} - 1,\ g^{ph} \equiv 1 \pmod{p^2},$$

if $h < \varphi(p)$, then $ph < \varphi(p^2)$, a contradiction. Thus $h = \varphi(p)$, g is a primitive root modulo p. □

Lemma 2.8. *Let g be a primitive root modulo p^l. Then g is a primitive root modulo $2p^l$, where g is odd and p and l are the same as mentioned above.*

Proof. Let s be the order of g modulo $2p^l$. Then

$$g^s \equiv 1 \pmod{2p^l},\ s|\varphi(2p^l).$$

So we have

$$g^s \equiv 1 \pmod{p^l}.$$

Since g is a primitive root modulo p^l, we have $\varphi(p^l)|s$ and hence $\varphi(2p^l)|s$. So

$$s = \varphi(2p^l)$$

and g is a primitive root modulo $2p^l$. □

3. Main result

Combining Lemmas 2.1 and 2.3, we can calculate the number of different irreducible factors for $x^n - 1$ over $\mathbb{F}_q$. Let m be a positive integer,

$$m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_l^{\alpha_l}$$

be its prime decomposition. If

$$n = mp^e,$$

where $e \geq 0$ is an integer, and p is the characteristic of $\mathbb{F}_q$ with $p \nmid m$. Then we can calculate that

$$|\mathfrak{F}(x^n - 1)| = \sum_{m'|m} \frac{\varphi(m')}{d_{m'}},$$

where $d_{m'}$ denotes the order of q modulo m'. Note that there are $\prod_{k=1}^{l}(\alpha_k + 1)$ items in the summation, where $\prod_{k=1}^{l}(\alpha_k + 1)$ is the number of factors of m.

Now assume that s and m are given positive integers, $m_1, \cdots, m_t$ are the t factors of m. Thus, we have

$$x^n - 1 = \prod_{i=1}^{t} \Phi_{m_i}(x)^{p^e}.$$

If $x^n - 1$ factors into s distinct irreducible polynomials in $\mathbb{F}_q[x]$, then

$$|\mathfrak{F}(x^n - 1)| = \sum_{i=1}^{t} \frac{\varphi(m_i)}{d_{m_i}} = s, \tag{3.1}$$

there are t items in the summation, the necessary and sufficient condition for

$$|\mathfrak{F}(x^n - 1)| = s$$

is determined as follows:

Observe $\frac{\varphi(m_i)}{d_{m_i}}$ $(i = 1, 2, \cdots, t)$, and $\varphi(m_i)$ are known; with the difference of q, the values of d_{m_i} will also change, that is, the values of $\frac{\varphi(m_i)}{d_{m_i}}$ will change in the different $\mathbb{F}_q$. Therefore, the t items in (3.1) can be regarded as t variables, and (3.1) can be regarded as the Diophantine equation with t variables

$$x_1 + x_2 + \cdots + x_t = s. \tag{3.2}$$

Remark 3.1. Combining Lemma 2.2 and Euler's theorem, we know that $\frac{\varphi(m_i)}{d_{m_i}}$ $(i = 1, 2, \cdots, t)$ are positive integers. So we only need to consider the positive integer solutions of (3.2).

Remark 3.2. The positive integers s and t satisfy $t \leq s$. Otherwise, if $t > s$, then it follows from Lemmas 2.1 and 2.3 that

$$|\mathfrak{F}(x^n - 1)| > s.$$

Remark 3.3. As we all know

$$\Phi_1(x) = x - 1$$

is a factor of $x^n - 1$, and $x - 1$ is irreducible over $\mathbb{F}_q$; the order of q modulo 1 is $d_1 = 1$. Thus, at least one positive integer solution of (3.2) whose value is 1.

We can find the positive integer solutions of (3.2). Without loss of generality, we suppose that

$$x_i = \frac{\varphi(m_i)}{d_{m_i}} = k_i \ (i = 1, 2, \cdots, t) \tag{3.3}$$

is the positive integer solution of (3.2), thus we have

$$d_{m_i} = \frac{\varphi(m_i)}{k_i} \ (i = 1, 2, \cdots, t). \tag{3.4}$$

If there exists q such that the order of q modulo m_i is

$$d_{m_i} = \frac{\varphi(m_i)}{k_i} \ (i = 1, 2, \cdots, t),$$

then it follows from Lemma 2.3 that $\Phi_{m_i}(x)$ factors into

$$\frac{\varphi(m_i)}{\frac{\varphi(m_i)}{k_i}} = k_i$$

distinct monic irreducible polynomials over $\mathbb{F}_q$ of the same degree

$$d_{m_i} = \frac{\varphi(m_i)}{k_i}.$$

Therefore, we have

$$|\mathfrak{F}(x^n - 1)| = k_1 + k_2 + \cdots + k_t = s,$$

that is, $x^n - 1$ factors into s distinct irreducible polynomials over $\mathbb{F}_q$.

In conclusion, we have the following result:

Theorem 3.4. (Main result) *Let $\mathbb{F}_q$ denote the finite field of q elements with characteristic p. Let p be a prime. Let*

$$n = mp^e$$

with $e \geq 0$, $p \nmid m$. Let s be a positive integer. The t factors of m are $m_1, m_2, \cdots, m_t$ and d_{m_i} denotes the order of q modulo m_i. Then

$$|\mathfrak{F}(x^n - 1)| = s,$$

if and only if

$$x_i = \frac{\varphi(m_i)}{d_{m_i}} \ (i = 1, 2, \cdots, t)$$

is a solution to the Diophantine equation

$$x_1 + x_2 + \cdots + x_t = s.$$

Proof. We first assume that

$$x_i = \frac{\varphi(m_i)}{d_{m_i}} = k_i \ (i = 1, 2, \cdots, t)$$

is the solution of the Diophantine equation

$$x_1 + x_2 + \cdots + x_t = s.$$

By Lemmas 2.1 and 2.3, we have

$$x^n - 1 = \prod_{i=1}^{t} \Phi_{m_i}(x)^{p^e}$$

and $\Phi_{m_i}(x)$ factors into

$$\frac{\varphi(m_i)}{\frac{\varphi(m_i)}{k_i}} = k_i$$

distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of the same degree

$$d_{m_i} = \frac{\varphi(m_i)}{k_i} \ (i = 1, 2, \cdots, t).$$

Hence, we obtain

$$|\mathfrak{F}(x^n - 1)| = \sum_{i=1}^{t} k_i = s.$$

Suppose

$$|\mathfrak{F}(x^n - 1)| = s.$$

According to Lemma 2.3, we have

$$|\mathfrak{F}(x^n - 1)| = \sum_{i=1}^{t} \frac{\varphi(m_i)}{d_{m_i}} = s.$$

So

$$x_i = \frac{\varphi(m_i)}{d_{m_i}} \ (i = 1, 2, \cdots, t)$$

is the solution of the Diophantine equation

$$x_1 + x_2 + \cdots + x_t = s.$$

□

4. Applications

We apply Theorem 3.4 to deduce Theorem 1.6. Note that Theorem 1.5 is trivial. Recall that

$$n = mp^e,$$

where $e \geq 0$ is an integer and p is the characteristic of $\mathbb{F}_q$ with $p \nmid m$.

For Theorem 1.6

$$|\mathfrak{F}(x^n - 1)| = 2,$$

we know that m has two factors; thus, m is a prime different from p,

$$x^n - 1 = (\Phi_1(x)\Phi_m(x))^{p^e}.$$

The unique positive integer solution of the Diophantine equation

$$x_1 + x_2 = 2$$

is

$$x_1 = x_2 = 1.$$

Since

$$\frac{\varphi(1)}{d_1} = 1,$$

and by Theorem 3.4, we have

$$\frac{\varphi(m)}{d_m} = 1,$$

that is, $d_m = \varphi(m)$, q is a primitive root modulo m. It follows from Lemma 2.5 that the cyclotomic polynomial $\Phi_m(x)$ is irreducible over $\mathbb{F}_q$. Thus

$$|\mathfrak{F}(x^n - 1)| = 2.$$

The necessary and sufficient conditions for

$$|\mathfrak{F}(x^n - 1)| = 3, 4, 5$$

are given, respectively, below: for

$$|\mathfrak{F}(x^n - 1)| = 3,$$

we know that $t \leq 3$, where t is the number of factors of m.

Case 1. If m has three factors, then $m = r^2$, where r is a prime different from p.

$$x^n - 1 = (\Phi_1(x)\Phi_r(x)\Phi_{r^2}(x))^{p^e}.$$

The unique positive integer solution of the Diophantine equation

$$x_1 + x_2 + x_3 = 3$$

is

$$x_1 = x_2 = x_3 = 1.$$

By Theorem 3.4, we have

$$\frac{\varphi(r)}{d_r} = 1, \quad \frac{\varphi(r^2)}{d_{r^2}} = 1,$$

that is,

$$d_r = \varphi(r), \quad d_{r^2} = \varphi(r^2),$$

q is a primitive root modulo r and r^2. Recall Lemma 2.7: If q is a primitive root modulo r^2, then q is a primitive root modulo r. Cyclotomic polynomials $\Phi_r(x)$ and $\Phi_{r^2}(x)$ are irreducible over $\mathbb{F}_q$. Thus

$$|\mathfrak{F}(x^n - 1)| = 3.$$

Case 2. If m has two factors, then $m = r$,

$$x^n - 1 = (\Phi_1(x)\Phi_r(x))^{p^e}.$$

The positive integer solution of the Diophantine equation

$$x_1 + x_2 = 3$$

is $x_1 = 1$, $x_2 = 2$. Hence, we obtain

$$\frac{\varphi(r)}{d_r} = 2,$$

that is,

$$d_r = \frac{\varphi(r)}{2},$$

the order of q modulo r is $\frac{\varphi(r)}{2}$. According to Lemma 2.3, the cyclotomic polynomial $\Phi_r(x)$ factors into

$$\frac{\varphi(r)}{\frac{\varphi(r)}{2}} = 2$$

distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of the same degree

$$d_r = \frac{\varphi(r)}{2}.$$

Thus

$$|\mathfrak{F}(x^n - 1)| = 3.$$

In conclusion, we have the following result:

Theorem 4.1. *The following statements are equivalent:*

(a) $|\mathfrak{F}(x^n - 1)| = 3$.

(b) (b1) $\mathfrak{F}(x^n - 1)=\{x - 1, f_1(x), f_2(x)\}$, *where* $m = r$,

$$f_1(x)f_2(x) = \Phi_r(x), \deg f_1 = \deg f_2 = \tfrac{\varphi(r)}{2}.$$

(b2) $\mathfrak{F}(x^n - 1)=\{x - 1, \Phi_r(x), \Phi_{r^2}(x)\}$, *where* $m = r^2$.

(c) (c1) $m = r$, *and the order of* q *modulo* r *is* $\frac{\varphi(r)}{2}$.

(c2) $m = r^2$, *and* q *is a primitive root modulo* r^2.

For

$$|\mathfrak{F}(x^n - 1)| = 4,$$

we know that $t \leq 4$, where t is the number of factors of m. In the remaining part of this paper, we always assume that r is an odd prime different from p.

If m has four factors, then the possible values of m are r^3, $2r$, p_1p_2 or 8, where p_1 and p_2 are odd primes different from p. The unique positive integer solution of the Diophantine equation

$$x_1 + x_2 + x_3 + x_4 = 4$$

is

$$x_1 = x_2 = x_3 = x_4 = 1.$$

Case 1. If $m = r^3$, then

$$x^n - 1 = (\Phi_1(x)\Phi_r(x)\Phi_{r^2}(x)\Phi_{r^3}(x))^{p^e},$$

and we have

$$\frac{\varphi(r)}{d_r} = \frac{\varphi(r^2)}{d_{r^2}} = \frac{\varphi(r^3)}{d_{r^3}} = 1,$$

that is, q is a primitive root modulo $r^l, l = 1, 2, 3$, which requires that q is a primitive root modulo r^2. The cyclotomic polynomials $\Phi_r(x)$, $\Phi_{r^2}(x)$, and $\Phi_{r^3}(x)$ are irreducible over $\mathbb{F}_q$. Thus

$$|\mathfrak{F}(x^n - 1)| = 4.$$

Case 2. If $m = 2r$, then

$$x^n - 1 = (\Phi_1(x)\Phi_2(x)\Phi_r(x)\Phi_{2r}(x))^{p^e},$$

and we have

$$\frac{\varphi(2)}{d_2} = \frac{\varphi(r)}{d_r} = \frac{\varphi(2r)}{d_{2r}} = 1,$$

that is, q is a primitive root modulo r and $2r$. Recall Lemma 2.8: If q is a primitive root modulo r, then q is a primitive root modulo $2r$. The cyclotomic polynomials $\Phi_r(x)$ and $\Phi_{2r}(x)$ are irreducible over $\mathbb{F}_q$. Obviously, the order of q modulo 2 is $d_2 = 1$, and

$$\Phi_2(x) = x + 1$$

is irreducible over $\mathbb{F}_q$. Thus

$$|\mathfrak{F}(x^n - 1)| = 4.$$

Case 3. If $m = p_1p_2$, then

$$x^n - 1 = (\Phi_1(x)\Phi_{p_1}(x)\Phi_{p_2}(x)\Phi_{p_1p_2}(x))^{p^e},$$

and we have

$$\frac{\varphi(p_1)}{d_{p_1}} = \frac{\varphi(p_2)}{d_{p_2}} = \frac{\varphi(p_1p_2)}{d_{p_1p_2}} = 1.$$

It follows from Lemma 2.4 that p_1p_2 has no primitive root, which contradicts

$$d_{p_1p_2} = \varphi(p_1p_2).$$

The cyclotomic polynomial $\Phi_{p_1p_2}(x)$ is reducible over $\mathbb{F}_q$. Thus

$$|\mathfrak{F}(x^n - 1)| > 4.$$

Case 4. If $m = 8$, then

$$x^n - 1 = (\Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x))^{p^e}.$$

Since 8 has no primitive root, $\Phi_8(x)$ is reducible over $\mathbb{F}_q$. Thus

$$|\mathfrak{F}(x^n - 1)| > 4.$$

If m has three factors, then the possible values of m are r^2 or 4. The positive integer solution of the equation

$$x_1 + x_2 + x_3 = 4$$

is

$$x_1 = x_2 = 1, x_3 = 2.$$

Case 1. If $m = r^2$, then

$$x^n - 1 = (\Phi_1(x)\Phi_r(x)\Phi_{r^2}(x))^{p^e},$$

and we have

$$\frac{\varphi(r)}{d_r} = 2, \quad \frac{\varphi(r^2)}{d_{r^2}} = 1$$

or

$$\frac{\varphi(r)}{d_r} = 1, \quad \frac{\varphi(r^2)}{d_{r^2}} = 2.$$

For the former, the order of q modulo r is

$$d_r = \frac{\varphi(r)}{2},$$

and q is a primitive root modulo r^2, which is impossible by Lemma 2.7. For the latter, q is a primitive root modulo r, and the order of q modulo r^2 is $\frac{\varphi(r^2)}{2}$. It follows that

$$q^{\varphi(r)} \equiv 1 \pmod{r}, \ q^{\frac{\varphi(r^2)}{2}} = q^{\frac{r\varphi(r)}{2}} \equiv 1 \pmod{r^2}, \ q^{\frac{r\varphi(r)}{2}} \equiv 1 \pmod{r}.$$

Thus $\varphi(r)|\frac{r\varphi(r)}{2}$. Since r is an odd prime, $\frac{r}{2}$ is not an integer, and the divisibility is not valid.

Case 2. If $m = 4$, then

$$x^n - 1 = (\Phi_1(x)\Phi_2(x)\Phi_4(x))^{p^e},$$

and we have

$$\frac{\varphi(4)}{d_4} = 2,$$

that is, the order of q modulo 4 is

$$d_4 = \frac{\varphi(4)}{2} = 1.$$

The cyclotomic polynomial

$$\Phi_4(x) = 1 + x^2$$

factors into

$$\frac{\varphi(4)}{\frac{\varphi(4)}{2}} = 2$$

distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of the same degree, $d_4 = 1$. Thus

$$|\mathfrak{F}(x^n - 1)| = 4.$$

If m has two factors, then $m = r$,

$$x^n - 1 = (\Phi_1(x)\Phi_r(x))^{p^e}.$$

The positive integer solution of the Diophantine equation

$$x_1 + x_2 = 4$$

is $x_1 = 1$, $x_2 = 3$. Hence, we have

$$\frac{\varphi(r)}{d_r} = 3,$$

that is, the order of q modulo r is $\frac{\varphi(r)}{3}$. The cyclotomic polynomial $\Phi_r(x)$ factors into three distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of the same degree $\frac{\varphi(r)}{3}$. Thus

$$|\mathfrak{F}(x^n - 1)| = 4.$$

In conclusion, we have the following result:

Theorem 4.2. *The following statements are equivalent:*

(a) $|\mathfrak{F}(x^n - 1)| = 4$.

(b) (b1) $\mathfrak{F}(x^n - 1)=\{x - 1, f_1(x), f_2(x), f_3(x)\}$, *where* $m = r$,

$$f_1(x)f_2(x)f_3(x) = \Phi_r(x), \deg f_1 = \deg f_2 = \deg f_3 = \frac{\varphi(r)}{3}.$$

(b2) $\mathfrak{F}(x^n - 1)=\{x - 1, \Phi_r(x), \Phi_{r^2}(x), \Phi_{r^3}(x)\}$, *where* $m = r^3$.

(b3) $\mathfrak{F}(x^n - 1)=\{x - 1, x + 1, \Phi_r(x), \Phi_{2r}(x)\}$, *where* $m = 2r$.

(b4) $\mathfrak{F}(x^n - 1)=\{x - 1, x + 1, x + e_1, x + e_2\}$, *where* $m = 4$, e_1 *and* e_2 *are integers.*

(c) (c1) $m = r$, *and the order of* q *modulo* r *is* $\frac{\varphi(r)}{3}$.

(c2) $m = r^3$, *and* q *is a primitive root modulo* r^2.

(c3) $m = 2r$, *and* q *is a primitive root modulo* r.

(c4) $m = 4$, *and the order of* q *modulo* 4 *is* 1.

For

$$|\mathfrak{F}(x^n - 1)| = 5,$$

we know that $t \leq 5$, where t is the number of factors of m.

If m has five factors, then the possible values of m are r^4 or 16. The unique positive integer solution of the equation

$$x_1 + x_2 + x_3 + x_4 + x_5 = 5$$

is

$$x_1 = x_2 = x_3 = x_4 = x_5 = 1.$$

Case 1. If $m = r^4$, then

$$x^n - 1 = (\Phi_1(x)\Phi_r(x)\Phi_{r^2}(x)\Phi_{r^3}(x)\Phi_{r^4}(x))^{p^e},$$

and we have

$$\frac{\varphi(r)}{d_r} = \frac{\varphi(r^2)}{d_{r^2}} = \frac{\varphi(r^3)}{d_{r^3}} = \frac{\varphi(r^4)}{d_{r^4}} = 1,$$

that is, q is a primitive root modulo $r^l, l = 1, 2, 3, 4$, which requires that q is a primitive root modulo r^2. The cyclotomic polynomials $\Phi_r(x), \Phi_{r^2}(x), \Phi_{r^3}(x)$, and $\Phi_{r^4}(x)$ are irreducible over $\mathbb{F}_q$. Thus

$$|\mathfrak{F}(x^n - 1)| = 5.$$

Case 2. If $m = 16$, then

$$x^n - 1 = (\Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x)\Phi_{16}(x))^{p^e}.$$

Since 8 and 16 have no primitive root, we know that $\Phi_8(x)$ and $\Phi_{16}(x)$ are reducible over $\mathbb{F}_q$. Thus

$$|\mathfrak{F}(x^n - 1)| > 5.$$

If m has four factors, then the possible values of m are $r^3, 8, 2r$ or p_1p_2. The positive integer solution of the equation

$$x_1 + x_2 + x_3 + x_4 = 5$$

is

$$x_1 = x_2 = x_3 = 1, x_4 = 2.$$

Case 1. If $m = r^3$, then

$$x^n - 1 = (\Phi_1(x)\Phi_r(x)\Phi_{r^2}(x)\Phi_{r^3}(x))^{p^e}.$$

It follows from Lemma 2.7 that

$$\frac{\varphi(r^2)}{d_{r^2}} = 2$$

and

$$\frac{\varphi(r)}{d_r} = \frac{\varphi(r^3)}{d_{r^3}} = 1,$$

that is, q is a primitive root modulo r^3, the order of q modulo r^2 is $\frac{\varphi(r^2)}{2}$. It follows that

$$q^{\varphi(r^3)} \equiv 1 \pmod{r^3},\ q^{\frac{\varphi(r^2)}{2}} \equiv 1 \pmod{r^2},\ q^{\frac{\varphi(r^2)}{2}} \equiv 1 \pmod{r}.$$

Since q is a primitive root modulo r^3, we have

$$v_r(q^{\frac{\varphi(r^2)}{2}} - 1) = 2.$$

By Lemma 2.6, we have

$$v_r(q^{r\frac{\varphi(r^2)}{2}} - 1) = v_r(q^{\frac{\varphi(r^2)}{2}} - 1) + v_r(r) = 2 + 1 = 3,$$

$$q^{\frac{\varphi(r^3)}{2}} \equiv 1(mod\ r^3),$$

which is a contradiction. Thus, if $m = r^3$, then

$$|\mathfrak{F}(x^n - 1)| \neq 5.$$

Case 2. If $m = 8$, then

$$x^n - 1 = (\Phi_1(x)\Phi_2(x)\Phi_4(x)\Phi_8(x))^{p^e},$$

and we have

$$\frac{\varphi(4)}{d_4} = 1,\ \ \frac{\varphi(8)}{d_8} = 2,$$

that is, q is a primitive root modulo 4, which means q is congruent to 3 modulo 4, therefore the order of q modulo 8 is

$$\frac{\varphi(8)}{2} = 2.$$

$\Phi_4(x)$ is irreducible over $\mathbb{F}_q$, and $\Phi_8(x)$ factors into

$$\frac{\varphi(8)}{\frac{\varphi(8)}{2}} = 2$$

distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of the same degree 2. Thus

$$|\mathfrak{F}(x^n - 1)| = 5.$$

Case 3. If $m = 2r$, then

$$x^n - 1 = (\Phi_1(x)\Phi_2(x)\Phi_r(x)\Phi_{2r}(x))^{p^e}.$$

It follows from Lemma 2.8 that

$$\frac{\varphi(r)}{d_r} = 2, \quad \frac{\varphi(2r)}{d_{2r}} = 1,$$

that is, q is a primitive root modulo $2r$, and the order of q modulo r is $\frac{\varphi(r)}{2}$, $\Phi_{2r}(x)$ is irreducible over $\mathbb{F}_q$ and $\Phi_r(x)$ factors into

$$\frac{\varphi(r)}{\frac{\varphi(r)}{2}} = 2$$

distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of the same degree $\frac{\varphi(r)}{2}$. Thus

$$|\mathfrak{F}(x^n - 1)| = 5.$$

Case 4. If $m = p_1p_2$, then

$$x^n - 1 = (\Phi_1(x)\Phi_{p_1}(x)\Phi_{p_2}(x)\Phi_{p_1p_2}(x))^{p^e}.$$

Since p_1p_2 has no primitive root, we have

$$\frac{\varphi(p_1)}{d_{p_1}} = \frac{\varphi(p_2)}{d_{p_2}} = 1, \quad \frac{\varphi(p_1p_2)}{d_{p_1p_2}} = 2,$$

that is, q is a primitive root modulo p_1 and p_2, and the order of q modulo p_1p_2 is $\frac{\varphi(p_1p_2)}{2}$, $\Phi_{p_1}(x)$ and $\Phi_{p_2}(x)$ are irreducible over $\mathbb{F}_q$, and $\Phi_{p_1p_2}(x)$ factors into

$$\frac{\varphi(p_1p_2)}{\frac{\varphi(p_1p_2)}{2}} = 2$$

distinct monic irreducible polynomials in $\mathbb{F}_q[x]$ of the same degree $\frac{\varphi(p_1p_2)}{2}$. Thus

$$|\mathfrak{F}(x^n - 1)| = 5.$$

If m has three factors, then the possible values of m are 4 or r^2. If $m = 4$, there are at most four distinct irreducible factors for $x^n - 1$. Thus

$$|\mathfrak{F}(x^n - 1)| < 5.$$

If $m = r^2$, then

$$x^n - 1 = (\Phi_1(x)\Phi_r(x)\Phi_{r^2}(x))^{p^e}.$$

The positive integer solutions of the equation

$$x_1 + x_2 + x_3 = 5$$

are

$$x_1 = 1, \ \ x_2 = x_3 = 2, \ \text{ or } \ x_1 = x_2 = 1, \ \ x_3 = 3.$$

For the former, we have

$$\frac{\varphi(r)}{d_r} = \frac{\varphi(r^2)}{d_{r^2}} = 2,$$

that is, the order of q modulo r is $\frac{\varphi(r)}{2}$ and the order of q modulo r^2 is $\frac{\varphi(r^2)}{2}$, $\Phi_r(x)$, and $\Phi_{r^2}(x)$ factor into 2 distinct monic irreducible polynomials in $\mathbb{F}_q[x]$. Thus

$$|\mathfrak{F}(x^n - 1)| = 5.$$

For the latter, it follows from Lemma 2.7 that

$$\frac{\varphi(r)}{d_r} = 1 \ \text{ and } \ \frac{\varphi(r^2)}{d_{r^2}} = 3,$$

that is, q is a primitive root modulo r, and the order of q modulo r^2 is $\frac{\varphi(r^2)}{3}$, $\Phi_r(x)$ is irreducible over $\mathbb{F}_q$ and $\Phi_{r^2}(x)$ factors into 3 distinct monic irreducible polynomials in $\mathbb{F}_q[x]$. Thus

$$|\mathfrak{F}(x^n - 1)| = 5.$$

If m has two factors, then

$$m = r, \ \ x^n - 1 = (\Phi_1(x)\Phi_r(x))^{p^e}.$$

The positive integer solution of the equation $x_1 + x_2 = 5$ is $x_1 = 1, x_2 = 4$. Hence, we have

$$\frac{\varphi(r)}{d_r} = 4,$$

that is, the order of q modulo r is $\frac{\varphi(r)}{4}$. The cyclotomic polynomial $\Phi_r(x)$ factors into four distinct monic irreducible polynomials in $\mathbb{F}_q[x]$. Thus

$$|\mathfrak{F}(x^n - 1)| = 5.$$

In conclusion, we obtain the following result:

Theorem 4.3. *The following statements are equivalent:*

(a) $|\mathfrak{F}(x^n - 1)| = 5$.

(b) (b1) $\mathfrak{F}(x^n - 1)=\{x - 1, \Phi_r(x), \Phi_{r^2}(x), \Phi_{r^3}(x), \Phi_{r^4}(x)\}$, *where* $m = r^4$.

(b2) $\mathfrak{F}(x^n - 1)=\{x - 1, x + 1, \Phi_4(x), f_1(x), f_2(x)\}$, *where* $m = 8$,

$$f_1(x)f_2(x) = \Phi_8(x), \ \deg f_1 = \deg f_2 = 2.$$

(b3) $\mathfrak{F}(x^n-1)=\{x-1, x+1, g_1(x), g_2(x), \Phi_{2r}(x)\}$, *where* $m=2r$,

$$g_1(x)g_2(x)=\Phi_r(x),\ \deg g_1=\deg g_2=\tfrac{\varphi(r)}{2}.$$

(b4) $\mathfrak{F}(x^n-1)=\{x-1, \Phi_{p_1}(x), \Phi_{p_2}(x), h_1(x), h_2(x)\}$, *where* $m=p_1p_2$,

$$h_1(x)h_2(x)=\Phi_{p_1p_2}(x),\ \deg h_1=\deg h_2=\tfrac{\varphi(p_1p_2)}{2}.$$

(b5) $\mathfrak{F}(x^n-1)=\{x-1, k_1(x), k_2(x), r_1(x), r_2(x)\}$, *where* $m=r^2$,

$k_1(x)k_2(x)=\Phi_r(x)$, $\deg k_1=\deg k_2=\frac{\varphi(r)}{2}$ *and* $r_1(x)r_2(x)=\Phi_{r^2}(x)$, $\deg r_1=\deg r_2=\frac{\varphi(r^2)}{2}$.

Or $\mathfrak{F}(x^n-1)=\{x-1, \Phi_r(x), u_1(x), u_2(x), u_3(x)\}$, *where* $m=r^2$,

$$u_1(x)u_2(x)u_3(x)=\Phi_{r^2}(x),\ \deg u_1=\deg u_2=\deg u_3=\tfrac{\varphi(r^2)}{3}.$$

(b6) $\mathfrak{F}(x^n-1)=\{x-1, v_1(x), v_2(x), v_3(x), v_4(x)\}$, *where* $m=r$,

$$v_1(x)v_2(x)v_3(x)v_4(x)=\Phi_r(x),\ \deg v_1=\deg v_2=\deg v_3=\deg v_4=\tfrac{\varphi(r)}{4}.$$

(c) (c1) $m=r^4$, *and* q *is a primitive root modulo* r^2.

(c2) $m=8$, q *is a primitive root modulo* 4, *and the order of* q *modulo* 8 *is* 2.

(c3) $m=2r$, *the order of* q *modulo* r *is* $\frac{\varphi(r)}{2}$ *and* q *is a primitive root modulo* $2r$.

(c4) $m=p_1p_2$, *the order of* q *modulo* p_1p_2 *is* $\frac{\varphi(p_1p_2)}{2}$, *and* q *is a primitive root modulo* p_1 *and* p_2.

(c5) $m=r^2$, *the order of* q *modulo* r *is* $\frac{\varphi(r)}{2}$ *and the order of* q *modulo* r^2 *is* $\frac{\varphi(r^2)}{2}$; *or* q *is a primitive root modulo* r *and the order of* q *modulo* r^2 *is* $\frac{\varphi(r^2)}{3}$.

(c6) $m=r$, *and the order of* q *modulo* r *is* $\frac{\varphi(r)}{4}$.

5. Examples

In this final section, we provide two examples.

Example 5.1. *Let* $\mathbb{F}_q$ *denote the finite field of* q *elements with characteristic* p. *Let* p *be a prime, let* r *be a prime different from* p, *and let* $n=r^lp^e$, *with* $l\geq 1$, $e\geq 0$. *Denote by* $\mathfrak{F}(x^n-1)$ *the set of all distinct monic irreducible factors of* x^n-1 *in a given finite field. Given a positive integer* s, *we consider the special case for*

$$|\mathfrak{F}(x^n-1)|=s=l+1.$$

Since $n=r^lp^e$,

$$x^n-1=(\Phi_1(x)\Phi_r(x)\Phi_{r^2}(x)\cdots\Phi_{r^l}(x))^{p^e}.$$

The unique positive integer solution of the equation

$$x_0+x_1+x_2+\cdots+x_l=l+1$$

is

$$x_i=\frac{\varphi(r^i)}{d_{r^i}}=1\ \ (i=0,1,\cdots,l),$$

where d_{r^i} denotes the order of q modulo r^i ($i = 0, 1, \cdots, l$). That is, q is a primitive root modulo r^j ($j = 1, 2, \cdots, l$). Recall Lemma 2.7 that if q is a primitive root modulo r^2, then q is a primitive root modulo r^j ($j = 1, 2, \cdots, l$). Cyclotomic polynomials $\Phi_{r^j}(x)$ ($j = 1, 2, \cdots, l$) are irreducible over $\mathbb{F}_q$.

In conclusion, if q is a primitive root modulo r^2, then

$$|\mathfrak{F}(x^{r^l p^e} - 1)| = l + 1.$$

Example 5.2. *We factor polynomial $x^{25} - 1$ into distinct monic irreducible polynomials over $\mathbb{F}_7$. Since $25 = 5^2$,*

$$x^{25} - 1 = x^{5^2} - 1 = \Phi_1(x)\Phi_5(x)\Phi_{25}(x).$$

We first calculate

$$7 \equiv 2 \pmod 5,\ \ 7^2 \equiv 4 \equiv -1 \pmod 5,\ \ 7^4 \equiv 1 \pmod 5,$$

where 7 is a primitive root modulo 5, thus

$$\Phi_5(x) = 1 + x + x^2 + x^3 + x^4$$

is irreducible over $\mathbb{F}_7$.

We next calculate

$$7 \equiv 7 \pmod{25},\quad 7^2 \equiv 24 \equiv -1 \pmod{25},\ \ 7^4 \equiv 1 \pmod{25},$$

the order of 7 modulo 25 is 4, thus

$$\Phi_{25}(x) = 1 + x^5 + x^{10} + x^{15} + x^{20}$$

factors into

$$\frac{\varphi(25)}{4} = 5$$

distinct monic irreducible polynomials over $\mathbb{F}_7$ of the same degree 4,

$$\begin{aligned}
f_1(x) &= 1 + 2x + 4x^2 + 2x^3 + x^4,\\
f_2(x) &= 1 + 4x + 4x^3 + x^4,\\
f_3(x) &= 1 + 4x + 3x^2 + 4x^3 + x^4,\\
f_4(x) &= 1 + 5x + 5x^2 + 5x^3 + x^4,\\
f_5(x) &= 1 + 6x + 5x^2 + 6x^3 + x^4,
\end{aligned}$$

respectively.

Thus

$$\begin{aligned}
x^{25} - 1 =&((x-1)(1 + x + x^2 + x^3 + x^4)(1 + 2x + 4x^2 + 2x^3 + x^4)(1 + 4x + 4x^3 + x^4)\\
&(1 + 4x + 3x^2 + 4x^3 + x^4)(1 + 5x + 5x^2 + 5x^3 + x^4)(1 + 6x + 5x^2 + 6x^3 + x^4))
\end{aligned}$$

and

$$|\mathfrak{F}(x^{25} - 1)| = 7.$$

6. Conclusions

Let $\mathbb{F}_q$ be the finite field of q elements, and $\mathbb{F}_{q^n}$ be its extension of degree n. Denote by $\mathfrak{F}(x^n - 1)$ the set of all distinct monic irreducible factors of the polynomial $x^n - 1$ in the finite field $\mathbb{F}_q$. Given a positive integer s, we use the properties of cyclotomic polynomials in finite fields and results from the Diophantine equations to provide the sufficient and necessary condition for

$$|\mathfrak{F}(x^n - 1)| = s.$$

As an application, we also obtain the sufficient and necessary conditions for

$$|\mathfrak{F}(x^n - 1)| = 3, 4, 5.$$

Author contributions

Weitao Xie: the first draft of the manuscript; Jiayu Zhang: preliminaries collection and analysis; Wei Cao: originally raised the problem and commented on previous versions of the manuscript. All authors contributed to the study conception and design. All authors read and approved the final manuscript.

Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

Acknowledgments

The authors thank the anonymous referees for their helpful comments that improved the quality of the manuscript. This work was jointly supported by the Fujian Provincial Natural Science Foundation of China (Grant No. 2022J02046), and Fujian Key Laboratory of Granular Computing and Applications (Minnan Normal University).

Conflict of interest

All authors declare no conflicts of interest in this paper.

References

1. J. H. Silverman, Taxicabs and sums of two cubes, *Amer. Math. Mon.*, **100** (1993), 331–340. http://doi.org/10.1080/00029890.1993.11990409
2. Z. G. Li, P. Z. Yuan, On the number of solutions of some special simultaneous Pell equations, *Acta Math. Sin. Chinese Ser.*, **50** (2007), 1349–1356.
3. B. Li, The solution structure of multivariate linear indeterminate equation and its application, *J. Anhui Univ.*, **39** (2015), 6–12. http://doi.org/10.3969/j.issn.1000-2162.2015.05.002

4. C. X. Zhu, Y. L. Feng, S. F. Hong, J. Y. Zhao, On the number of zeros of to the equaton $f(x_1) + \cdots + f(x_n) = a$ over finite fields, *Finite Fields Their Appl.*, **76** (2021), 101922. https://doi.org/10.1016/j.ffa.2021.101922
5. J. Y. Zhao, Y. Zhao, Y. J. Niu, On the number of solutions of two-variable diagonal quartic equations over finite fields, *AIMS Math.*, **5** (2020), 2979–2991. https://doi.org/10.3934/math.2020192
6. S. Perlis, Normal bases of cyclic fields of prime-power degree, *Duke Math. J.*, **9** (1942), 507–517. http://doi.org/10.1215/S0012-7094-42-00938-4
7. D. Pei, C. Wang, J. Omura, Normal basis of finite field $GF(2^m)$, *IEEE Trans. Inf. Theory*, **32** (1986), 285–287. http://doi.org/10.1109/TIT.1986.1057152
8. Y. Chang, T. K. Truong, I. S. Reed, Normal bases over $GF(q)$, *J. Algebra*, **241** (2001), 89–101. https://doi.org/10.1006/jabr.2001.8765
9. H. Huang, S. M. Han, W. Cao, Normal bases and irreducible polynomials, *Finite Fields Their Appl.*, **50** (2018), 272–278. https://doi.org/10.1016/j.ffa.2017.12.004
10. S. H. Gao, *Normal bases over finite fields*, University of Waterloo, 1993.
11. W. Cao, Normal bases and factorization of $x^n - 1$ in finite fields, *Appl. Algebra Eng. Commun. Comput.*, **35** (2024), 167–175. http://doi.org/10.1007/s00200-022-00540-z
12. R. Lidl, H. Niederreiter, *Finite fields*, Cambridge University Press, 1997. http://doi.org/10.1017/CBO9780511525926
13. Z. Ke, Q. Sun, *Lectures on number theory*, Higher Education Press, 2001.
14. K. Ireland, M. Rosen, *A classical introduction to modern number theory*, Springer-Verlag, 1990. https://doi.org/10.1007/978-1-4757-2103-4
15. A. H. Parvardi, Lifting the exponent lemma (LTE), Art of Problem Solving, 2011.

AIMS Press