Mathematics

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

AIMS Mathematics, 9(8): 21656–21671.
DOI: 10.3934/math.20241053
Received: 10 May 2024
Revised: 22 June 2024
Accepted: 28 June 2024
Published: 08 July 2024

Research article

A note on some diagonal cubic equations over finite fields

Wenxu Ge[1,*], **Weiping Li**[2,3] **and Tianze Wang**[3]

[1] School of Mathematics and Statistics, North China University of Water Resources and Electric Power, Zhengzhou 450046, China
[2] School of Mathematics and Information Sciences, Henan University of Economics and Law, Zhengzhou 450046, China
[3] Institute of Mathematics, Henan Academy of Sciences, Zhengzhou 450046, China

* **Correspondence:** Email: gewenxu@ncwu.edu.cn.

Abstract: Let a prime $p \equiv 1(\text{mod}3)$ and z be non-cubic in $\mathbb{F}_p$. Gauss proved that the number of solutions of equation

$$x_1^3 + x_2^3 + zx_3^3 = 0$$

in $\mathbb{F}_p$ was $p^2 + \frac{1}{2}(p-1)(9d-c)$, where c was uniquely determined and d, except for the sign, was defined by

$$4p = c^2 + 27d^2, \quad c \equiv 1(\text{mod}3).$$

In 1978, Chowla, Cowles, and Cowles determined the sign of d for the case of 2 being non-cubic in $\mathbb{F}_p$. In this paper, we extended the result of Chowla, Cowles and Cowles to finite field $\mathbb{F}_q$ with $q = p^k$, $p \equiv 1(\text{mod}3)$, and determined the sign of d for the case of 3 being non-cubic.

Keywords: Gauss sum; finite field; diagonal cubic equation
Mathematics Subject Classification: 11T23, 11T24

1. Introduction

Let $\mathbb{F}_q$ be a finite field of

$$q = p^k$$

elements. Let $\mathbb{F}_q^*$ be the multiplicative group of $\mathbb{F}_q$, i.s.,

$$\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}.$$

Counting the number of solutions $(x_1, x_2, \cdots, x_n) \in \mathbb{F}_q^n$ of the general diagonal equation

$$a_1x_1^{d_1} + a_2x_2^{d_2} + \cdots + a_nx_n^{d_n} = b$$

over $\mathbb{F}_q$ is an important and fundamental problem in number theory and finite field. The special case where all the d_i are equal has extensively been studied by many authors (see, for example, [1–3] for $d_i = 3$, and [4,5] for $d_i = 4$).

For a prime

$$p \equiv 1(\text{mod}3),$$

Chowla et al. [6–8] first considered the number of solutions of equation

$$x_1^3 + x_2^3 + zx_3^3 = 0 \tag{1.1}$$

over finite field $\mathbb{F}_p$.

For z is cubic, using the classic result of the cubic equation of periods by Gauss [9]. Chowla et al. [10] showed that the number of solutions of (1.1) is $p^2 + c(p-1)$, where c is uniquely determined by

$$4p = c^2 + 27d^2, \quad c \equiv 1(\text{mod}3). \tag{1.2}$$

For z is non-cubic, as pointed out in [6], using the classic result of the cubic equation of periods by Gauss [9], one can only obtain that the number of solutions of (1.1) is

$$p^2 + \frac{1}{2}(p-1)(9d-c),$$

where c is uniquely determined, and d is determined except for the sign by

$$4p = c^2 + 27d^2, \quad c \equiv 1(\text{mod}3).$$

Thus the key of these problems is to determine the sign of d. Chowla et al. [6] determined the sign of d for the case of 2 being non-cubic in $\mathbb{F}_p$.

Theorem 1.1. *[6] Let a prime be*

$$p \equiv 1(\text{mod}3).$$

If 2 is non-cubic in $\mathbb{F}_p$, then for any non-cubic element z, the number of solutions of (1.1) is

$$p^2 + \frac{1}{2}(p-1)(9d-c),$$

where c and d are uniquely determined by (1.2) with

$$d \equiv \begin{cases} c(\text{mod}4), & \text{if } z \equiv 2(\text{mod}H), \\ -c(\text{mod}4), & \text{if } z \equiv 4(\text{mod}H), \end{cases}$$

where H is the subgroup of nonzero cubes in $\mathbb{F}_p^*$.

Therefore, it is nature to ask the following problem: Is there another element which can determine the sign of d?

In this paper, we extend the result of Chowla et al. to finite field $\mathbb{F}_q$, and determine the sign of d by non-cube 3.

In the rest of this paper, $\mathbb{F}_q$ is a finite field of

$$q = p^k$$

elements with

$$p \equiv 1 (\bmod 3),$$

and $\mathbb{F}_q^*$ is the multiplicative group of $\mathbb{F}_q$, i.s.,

$$\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}.$$

For any $z \in \mathbb{F}_q$, one lets $A_n(z)$ denote the number of solutions of the following diagonal equation

$$x_1^3 + x_2^3 + \cdots + x_n^3 = z$$

over $\mathbb{F}_q$. Let $B_n(z)$ be the number of solutions of diagonal cubic equation

$$x_1^3 + x_2^3 + \cdots + x_n^3 + z x_{n+1}^3 = 0$$

over $\mathbb{F}_q$. Since

$$p \equiv 1 (\bmod 3),$$

the nonzero cubic elements form a multiplicative subgroup H of order $\frac{1}{3}(q-1)$ and index 3, which partitions $\mathbb{F}_q^*$ into three cosets H, zH and z^2H. Now, we can state our main results.

Theorem 1.2. *Let $\mathbb{F}_q$ be a finite field of*

$$q = p^k$$

elements with the prime

$$p \equiv 1 (\bmod 3).$$

c is uniquely determined, and d is determined except for the sign by

$$4q = c^2 + 27d^2, \quad c \equiv 1 (\bmod 3), \quad (c, p) = 1. \tag{1.3}$$

(1) If $2 \mid d$, then 2 is a cube in $\mathbb{F}_q$ and one has

$$A_2(2) = q - 2 + c, \quad B_2(2) = q^2 + c(q-1).$$

(2) If $2 \nmid d$, then 2 is a non-cube in $\mathbb{F}_q$, and for any non-cubic z, one has

$$A_2(z) = \begin{cases} q - 2 + \frac{1}{2}(9d - c), & \text{if } z \equiv 2 (\bmod H), \\ q - 2 + \frac{1}{2}(-9d - c), & \text{if } z \equiv 4 (\bmod H), \end{cases}$$

and

$$B_2(z) = \begin{cases} q^2 + \frac{1}{2}(q-1)(9d - c), & \text{if } z \equiv 2 (\bmod H), \\ q^2 + \frac{1}{2}(q-1)(-9d - c), & \text{if } z \equiv 4 (\bmod H), \end{cases}$$

where d is uniquely determined by (1.3) and

$$d \equiv c (\bmod 4).$$

Theorem 1.3. *Let $\mathbb{F}_q$ be a finite field of*

$$q = p^k$$

elements with the prime

$$p \equiv 1 (\text{mod} 3).$$

c is uniquely determined, and d is determined except for the sign by (1.3).

(1) If $3 \mid d$, then 3 is a cube in $\mathbb{F}_q$, and one has

$$A_2(3) = q - 2 + c \quad \textit{and} \quad B_2(3) = q^2 + c(q-1).$$

(2) If $3 \nmid d$, then 3 is a non-cube in $\mathbb{F}_q$, and for any non-cubic z, one has

$$A_2(z) = \begin{cases} q - 2 + \frac{1}{2}(9d - c), & \textit{if } z \equiv 3 (\text{mod} H), \\ q - 2 + \frac{1}{2}(-9d - c), & \textit{if } z \equiv 9 (\text{mod} H), \end{cases}$$

and

$$B_2(z) = \begin{cases} q^2 + \frac{1}{2}(q-1)(9d - c), & \textit{if } z \equiv 3 (\text{mod} H), \\ q^2 + \frac{1}{2}(q-1)(-9d - c), & \textit{if } z \equiv 9 (\text{mod} H), \end{cases}$$

where d is uniquely determined by (1.3) and $d \equiv -1 (\text{mod} 3)$.

Remark 1.4. (1) When z is cubic in $\mathbb{F}_q$ with

$$p \equiv 1 (\text{mod} 3),$$

as pointed out in [11] (or [12]), one has

$$A_2(z) = q - 2 + c \quad \text{and} \quad B_2(z) = q^2 + c(q-1).$$

(2) When

$$q \equiv 2 (\text{mod} 3),$$

it is known that every element is a cube. When

$$q \equiv 1 (\text{mod} 3)$$

with

$$p \equiv 2 (\text{mod} 3),$$

as [13, Theorem 16], one has

$$c = \begin{cases} -2p^{k/2}, & \text{if } k \equiv 0 (\text{mod} 4), \\ 2p^{k/2}, & \text{if } k \equiv 2 (\text{mod} 4), \end{cases}$$

and $d = 0$.

(3) In [12], Hong and Zhu use the generator g of group $\mathbb{F}_q^*$ to determine the sign of d, and give the sign of d by

$$\delta_z(q) = \begin{cases} (-1)^{\langle ind_g(d)\rangle_3} \cdot sgn\left(\mathrm{Im}(r_1 + 3\sqrt{3}r_2\mathrm{i})^k\right), & \text{if } k \equiv 1(\mathrm{mod}2), \\ 0, & \text{if } k \equiv 0(\mathrm{mod}2), \end{cases} \tag{1.4}$$

where r_1 and r_2 are uniquely determined by

$$4p = r_1^2 + 27r_2^2, \ \ r_1 \equiv 1(\mathrm{mod}3), \ \ 9r_2 \equiv (2\mathrm{N}_{\mathbb{F}_q/\mathbb{F}_p}(g)^{\frac{p-1}{3}} + 1)r_1(\mathrm{mod}p).$$

Here, the norm $\mathrm{N}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)$ of $\alpha \in \mathbb{F}_q$ over $\mathbb{F}_p$ is defined by

$$\mathrm{N}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) = \alpha \times \alpha^p \times \cdots \times \alpha^{p^{k-1}} = \alpha^{\frac{q-1}{p-1}}.$$

Recently, the authors [14] determined the sign of d by

$$4q = c^2 + 27d^2, \ \ c \equiv 1(\mathrm{mod}3), \ \ (c, p) = 1, \ \ 9d \equiv c(2z^{\frac{q-1}{3}} + 1)(\mathrm{mod}p). \tag{1.5}$$

In this paper, we give a more effective way to determine the sign of d for the cases of 2 or 3 being non-cubic.

Using the author's methods in [14] and Theorems 1.2 and 1.3, we immediately obtain the following corollaries:

Corollary 1.5. *Let $\mathbb{F}_q$ be a finite field of*

$$q = p^k$$

elements with the prime

$$p \equiv 1(\mathrm{mod}3).$$

c is uniquely determined, and d is determined except for the sign by (1.3). If $2 \nmid d$, then for any non-cubic element z, one has

$$\sum_{n=1}^{\infty} A_n(z)x^n = \begin{cases} \frac{x}{1-qx} - \frac{x+\frac{1}{2}(4+c-9d)x^2+cx^3}{1-3qx^2-qcx^3}, & \textit{if } z \equiv 2(\mathrm{mod}H), \\ \frac{x}{1-qx} - \frac{x+\frac{1}{2}(4+c+9d)x^2+cx^3}{1-3qx^2-qcx^3}, & \textit{if } z \equiv 4(\mathrm{mod}H), \end{cases}$$

and

$$\sum_{n=1}^{\infty} B_n(z)x^n = \begin{cases} \frac{1}{1-qx} - \frac{(q-1)x+\frac{1}{2}(q-1)(c-9d)x^2}{1-3qx^2-qcx^3}, & \textit{if } z \equiv 2(\mathrm{mod}H), \\ \frac{1}{1-qx} - \frac{(q-1)x+\frac{1}{2}(q-1)(c+9d)x^2}{1-3qx^2-qcx^3}, & \textit{if } z \equiv 4(\mathrm{mod}H), \end{cases}$$

where d is uniquely determined by (1.3) and

$$d \equiv c(\mathrm{mod}4).$$

Corollary 1.6. *Let $\mathbb{F}_q$ be a finite field of*

$$q = p^k$$

elements with the prime

$$p \equiv 1(\mathrm{mod}3).$$

c is uniquely determined, and d is determined except for the sign by (1.3). If $3 \nmid d$*, then for any non-cubic element z, one has*

$$\sum_{n=1}^{\infty} A_n(z)x^n = \begin{cases} \frac{x}{1-qx} - \frac{x+\frac{1}{2}(4+c-9d)x^2+cx^3}{1-3qx^2-qcx^3}, & \text{if } z \equiv 3(\mathrm{mod}H), \\ \frac{x}{1-qx} - \frac{x+\frac{1}{2}(4+c+9d)x^2+cx^3}{1-3qx^2-qcx^3}, & \text{if } z \equiv 9(\mathrm{mod}H), \end{cases}$$

and

$$\sum_{n=1}^{\infty} B_n(z)x^n = \begin{cases} \frac{1}{1-qx} - \frac{(q-1)x+\frac{1}{2}(q-1)(c-9d)x^2}{1-3qx^2-qcx^3}, & \text{if } z \equiv 3(\mathrm{mod}H), \\ \frac{1}{1-qx} - \frac{(q-1)x+\frac{1}{2}(q-1)(c+9d)x^2}{1-3qx^2-qcx^3}, & \text{if } z \equiv 9(\mathrm{mod}H), \end{cases}$$

where d is uniquely determined by (1.3) and

$$d \equiv -1(\mathrm{mod}3).$$

2. Auxiliary lemmas

Lemma 2.1. *[15] Let* $\mathbb{F}_q$ *be a finite field. Let* ψ *be a nontrivial additive character of* $\mathbb{F}_q$*. Then, for any* $a \in \mathbb{F}_q$*, we have*

$$\sum_{x\in\mathbb{F}_q} \psi(ax) = \begin{cases} q, & \text{if } a = 0, \\ 0, & \text{if } a \neq 0. \end{cases}$$

For any $a \in \mathbb{F}_q^*$, we defined the Gauss sums

$$S_a = \sum_{x\in\mathbb{F}_q} \psi(ax^3).$$

Lemma 2.2. *[13] Let* $\mathbb{F}_q$ *be the finite field of* $q = p^k$ *elements with the prime*

$$p \equiv 1(\mathrm{mod}3),$$

and z is non-cubic in $\mathbb{F}_q^*$*. Then,* S_1*,* S_z*, and* S_{z^2} *are the roots of the cubic equation*

$$x^3 - 3qx - qc = 0,$$

where c is uniquely determined by

$$4q = c^2 + 27d^2, \quad c \equiv 1(\mathrm{mod}3), \quad (c, p) = 1. \tag{2.1}$$

Lemma 2.3. *With the conditions of Lemma 2.2, one has*

$$A_n(z) = q^{n-1} + \frac{1}{3q}(S_1^n S_z + S_z^n S_{z^2} + S_{z^2}^n S_1 - S_1^n - S_z^n - S_{z^2}^n).$$

Proof. Since

$$p \equiv 1 (\mathrm{mod} 3),$$

the nonzero cubic elements form a multiplicative subgroup H of order $\frac{1}{3}(q-1)$ and index 3, which partitions $\mathbb{F}_q^*$ into three cosets H, zH, and z^2H. Then, for any $a \in z^jH$, we have

$$S_a = S_{z^j} \text{ and } S_{az} = S_{z^{j+1}}.$$

For any $b \in \mathbb{F}_q^*$, we have

$$\begin{aligned} S_b &= \sum_{x\in\mathbb{F}_q} \psi(bx^3) \\ &= 1 + \sum_{x\in\mathbb{F}_q^*} \psi(bx^3) \\ &= 1 + 3\sum_{a\in H} \psi(ab). \end{aligned}$$

Thus, we have

$$\sum_{a\in H} \psi(ab) = \frac{1}{3}(S_b - 1).$$

Then, by Lemma 2.1, we have

$$\begin{aligned} A_n(z) &= \frac{1}{q}\sum_{a\in\mathbb{F}_q} \sum_{(x_1,x_2,\cdots,x_n)\in\mathbb{F}_q^n} \psi(a(x_1^3 + \cdots + x_n^3 - z)) \\ &= q^{n-1} + \frac{1}{q}\sum_{a\in\mathbb{F}_q} \psi(-az)S_a^n \\ &= q^{n-1} + \frac{1}{q}\left(S_1^n \sum_{a\in H}\psi(-az) + S_z^n \sum_{a\in zH}\psi(-az) + S_{z^2}^n \sum_{a\in z^2H}\psi(-az)\right) \\ &= q^{n-1} + \frac{1}{q}\left(S_1^n \sum_{a\in H}\psi(-az) + S_z^n \sum_{a\in H}\psi(-az^2) + S_{z^2}^n \sum_{a\in H}\psi(-az^3)\right) \\ &= q^{n-1} + \frac{1}{3q}\left(S_1^n(S_{-z} - 1) + S_z^n(S_{-z^2} - 1) + S_{z^2}^n(S_{-z^3} - 1)\right) \\ &= q^{n-1} + \frac{1}{3q}\left(S_1^n(S_1 - 1) + S_z^n(S_{z^2} - 1) + S_{z^2}^n(S_1 - 1)\right) \\ &= q^{n-1} + \frac{1}{3q}(S_1^nS_z + S_z^nS_{z^2} + S_{z^2}^nS_1 - S_1^n - S_z^n - S_{z^2}^n), \end{aligned}$$

since -1 is cubic in $\mathbb{F}_q^*$. □

Lemma 2.4. *With the conditions of Lemma 2.2, one has*

$$A_3(z) = q^2 - 3q - c,$$

where c is uniquely determined by (2.1).

Proof. By lemma 2.2, we have

$$S_1 S_z + S_z S_{z^2} + S_{z^2} S_1 = -3q,\ S_1 + S_z + S_{z^2} = 0$$

and

$$S_{z^j} = 3qS_{z^j} + qc, \quad j = 0, 1, 2.$$

Then, by Lemma 2.3, we have

$$\begin{aligned} A_3(z) &= q^2 + \frac{1}{3q}(S_1^3 S_z + S_z^3 S_{z^2} + S_{z^2}^3 S_1 - S_1^3 - S_z^3 - S_{z^2}^3) \\ &= q^2 + \frac{1}{3q}\left[3q(S_1 S_z + S_z S_{z^2} + S_{z^2} S_1) + q(c-3)(S_1 + S_z + S_{z^2}) - 3qc\right] \\ &= q^2 - 3q - c. \end{aligned}$$

□

Lemma 2.5. *With the conditions of Lemma 2.2, one has $A_2(z)$ as one of the values*

$$q - 2 + \frac{1}{2}(\pm 9d - c),$$

and $A_2(z^2)$ is the other, where c is uniquely determined, and d is determined except for the sign by (2.1).

Proof. Similar to the proof of Lemma 2.4, we have

$$A_2(z) = q - 2 + \frac{1}{3q}(S_1^2 S_z + S_z^2 S_{z^2} + S_{z^2}^2 S_1), \tag{2.2}$$

$$A_2(z^2) = q - 2 + \frac{1}{3q}(S_1^2 S_{z^2} + S_z^2 S_1 + S_{z^2}^2 S_z). \tag{2.3}$$

By Lemma 2.2, we have

$$\begin{aligned} &S_1^2 S_z + S_z^2 S_{z^2} + S_{z^2}^2 S_1 + S_1^2 S_{z^2} + S_z^2 S_1 + S_{z^2}^2 S_z \\ &= (S_1 S_z + S_z S_{z^2} + S_{z^2} S_1)(S_1 + S_z + S_{z^2}) - 3S_1 S_z S_{z^2} \\ &= -3qc \end{aligned} \tag{2.4}$$

and

$$\begin{aligned} &[S_1^2 S_z + S_z^2 S_{z^2} + S_{z^2}^2 S_1 - (S_1^2 S_{z^2} + S_z^2 S_1 + S_{z^2}^2 S_z)]^2 \\ &= (S_1 - S_z)^2 (S_z - S_{z^2})^2 (S_{z^2} - S_1)^2 \\ &= -(4(-3q)^3 + 27(-qc)^2) \\ &= 27q^2(4q - c^2) \\ &= (27qd)^2. \end{aligned} \tag{2.5}$$

Then Lemma 2.5 follows from (2.2)–(2.5).

□

Lemma 2.6. *We have*

$$B_2(z) = (q-1)A_2(z) + 3q - 2.$$

Proof. By the definition of $B_2(z)$ and $A_2(z)$, we have

$$\begin{aligned} B_2(z) &= \sum_{\substack{(x_1,x_2,x_3)\in\mathbb{F}_q^3 \\ x_1^3+x_2^3+zx_3^3=0}} 1 \\ &= \sum_{x_3\in\mathbb{F}_q^*} \sum_{\substack{(x_1,x_2)\in\mathbb{F}_q^2 \\ x_1^3+x_2^3+zx_3^3=0}} 1 + \sum_{\substack{(x_1,x_2)\in\mathbb{F}_q^2 \\ x_1^3+x_2^3=0}} 1 \\ &= \sum_{x_3\in\mathbb{F}_q^*} \sum_{\substack{(x_1,x_2)\in\mathbb{F}_q^2 \\ x_1^3+x_2^3=z}} 1 + 3q - 2 \\ &= (q-1)A_2(z) + 3q - 2. \end{aligned}$$

□

Lemma 2.7. *Let $\mathbb{F}_q$ be the finite field of*

$$q = p^k$$

elements with the prime

$$p \equiv 1(\mathrm{mod}3).$$

c is uniquely determined, and d is determined except for the sign by (1.3). Then, 2 is a cube in $\mathbb{F}_q^*$ if, and only if, $2 \mid d$; 3 is a cube in $\mathbb{F}_q^*$ if, and only if, $3 \mid d$.

Proof. Since $\mathbb{F}_q^*$ is a cyclic group, 2 is cubic in $\mathbb{F}_q^*$ if, and only if,

$$2^{\frac{q-1}{3}} \equiv 1(\mathrm{mod}\, p).$$

By the Euler theorem, we have

$$2^{p-1} \equiv 1(\mathrm{mod}\, p).$$

Note that

$$q = p^k \quad \text{and} \quad p \equiv 1(\mathrm{mod}3),$$

then we have

$$2^{\frac{q-1}{3}} \equiv 2^{\frac{p-1}{3}(1+p+p^2+\cdots+p^{k-1})} \equiv 2^{\frac{k(p-1)}{3}}(\mathrm{mod}\, p).$$

By [16, Theorem 7.1.1], 2 is cubic in $\mathbb{F}_p$ if, and only if, $2 \mid d_0$, where c_0 and d_0 are determined by

$$4p = c_0^2 + 27d_0^2, \quad c_0 \equiv 1(\mathrm{mod}3).$$

That is,

$$2^{\frac{p-1}{3}} \equiv 1(\mathrm{mod}\, p),$$

if, and only if, $2 \mid d_0$. Thus, we have that 2 is cubic in $\mathbb{F}_q^*$ if, and only if, $2 \mid d_0$ or $3 \mid k$.

Next, we will prove that $2 \mid d_0$ or $3 \mid k$ if, and only if, $2 \mid d$. Since

$$4q = c^2 + 27d^2,$$

we have $2 \mid c$ if, and only if, $2 \mid d$. As pointed out in [14, Lemma 2.8], in integeral ring O_K of cubic cyclotomic field

$$K = \mathbb{Q}(\omega), \quad \omega = \frac{-1 + \sqrt{3}\mathrm{i}}{2},$$

we have

$$\frac{c + 3\sqrt{3}d\mathrm{i}}{2} = (-1)^{k-1}\left(\frac{c_0 + 3\sqrt{3}d_0\mathrm{i}}{2}\right)^k.$$

So, we have

$$\begin{aligned} c &= (-1)^{k-1}\left(\frac{c_0 + 3\sqrt{3}d_0\mathrm{i}}{2}\right)^k + (-1)^{k-1}\left(\frac{c_0 - 3\sqrt{3}d_0\mathrm{i}}{2}\right)^k \\ &= (-1)^{k-1}\left(\frac{c_0 + 3d_0}{2} + 3d_0\omega\right)^k + (-1)^{k-1}\left(\frac{c_0 + 3d_0}{2} + 3d_0\overline{\omega}\right)^k. \end{aligned}$$

If $2 \mid d_0$, it is easy to see that $2 \mid c$. If $2 \nmid d_0$, then $2 \mid \frac{c_0+3d_0}{2}$ or $2 \mid \frac{c_0-3d_0}{2}$, since

$$4p = c_0^2 + 27d_0^2.$$

When $2 \mid \frac{c_0+3d_0}{2}$, we have

$$c \equiv (3d_0)^k(\omega^k + \overline{\omega}^k) \equiv \omega^k + \overline{\omega}^k (\bmod 2).$$

When $2 \mid \frac{c_0-3d_0}{2}$, we have

$$\begin{aligned} c &= (-1)^{k-1}\left(\frac{c_0 + 3\sqrt{3}d_0\mathrm{i}}{2}\right)^k + (-1)^{k-1}\left(\frac{c_0 - 3\sqrt{3}d_0\mathrm{i}}{2}\right)^k \\ &= (-1)^{k-1}\left(\frac{c_0 - 3d_0}{2} - 3d_0\overline{\omega}\right)^k + (-1)^{k-1}\left(\frac{c_0 - 3d_0}{2} - 3d_0\omega\right)^k. \end{aligned}$$

Thus we have

$$c \equiv (-3d_0)^k(\omega^k + \overline{\omega}^k) \equiv \omega^k + \overline{\omega}^k (\bmod 2).$$

Hence, we have 2 is cubic in $\mathbb{F}_q^*$ if, and only if, $2 \mid d_0$, or $3 \mid k$ if, and only if, $2 \mid c$, or if and only if $2 \mid d$. Similarly, we can also prove that 3 is a cube in $\mathbb{F}_q^*$ if, and only if, $3 \mid d$. □

3. Proof of Theorem 1.2

Let $\mathbb{F}_q$ be a finite field of

$$q = p^k$$

elements with

$$p \equiv 1 (\bmod 3).$$

Then the nonzero cubic elements form a multiplicative subgroup H of order $\frac{1}{3}(q-1)$. We let

$$\mathcal{M} = \{(a, b) \in H^2 | a + b = 2\} \quad \text{and} \quad M = |\mathcal{M}|.$$

Since for any $a \in H$, the equation $x^3 = a$ in $\mathbb{F}_q$ exactly has three different solutions, if 2 is non-cubic in $\mathbb{F}_q^*$, then it is easy to see that

$$9M = A_2(2). \tag{3.1}$$

Lemma 3.1. *If 2 and z are non-cubic in $\mathbb{F}_q^*$, then*

$$A_2(z) = \begin{cases} A_2(2), & \text{if } z \equiv 2(\text{mod} H), \\ A_2(4), & \text{if } z \equiv 4(\text{mod} H). \end{cases}$$

Proof. Since 2 and z are non-cubic in $\mathbb{F}_q^*$, $z \in 2H \cup 4H$. If $z \in 2H$, i.e.,

$$z \equiv 2(\text{mod} H),$$

there is a $h \in \mathbb{F}_q^*$ and $z = 2h^3$. Then, it is easy to see that

$$A_2(z) = \sum_{\substack{(x_1,x_2)\in\mathbb{F}_q^2 \\ x_1^3+x_2^3=z}} 1 = \sum_{\substack{(x_1,x_2)\in\mathbb{F}_q^2 \\ x_1^3+x_2^3=2h^3}} 1 = \sum_{\substack{(x_1,x_2)\in\mathbb{F}_q^2 \\ (x_1h^{-1})^3+(x_2h^{-1})^3=2}} 1 = A_2(2).$$

Similarly, if

$$z \equiv 4(\text{mod} H),$$

we have

$$A_2(z) = A_2(4).$$

□

Lemma 3.2. *We have* $M \equiv 1(\text{mod} 2)$.

Proof. Let

$$\mathcal{M}_1 = \{(a, b) \in H^2 | a + b = 2, a \neq b\} \quad \text{and} \quad M_1 = |\mathcal{M}_1|.$$

Obviously, if $(a, b) \in \mathcal{M}_1$, then $(b, a) \in \mathcal{M}_1$. Thus, we have M_1 is even. If $(a, a) \in \mathcal{M}$, then $a = 1$. Hence, M is odd. □

Proof of Theorem 1.2. If $2 \mid d$, then 2 is a cube in $\mathbb{F}_q$ by Lemma 2.7, and one has

$$A_2(2) = q - 2 + c \quad \text{and} \quad B_2(2) = q^2 + c(q - 1)$$

as pointed out in [11] (or [12]).

If $2 \nmid d$, then 2 is non-cubic in $\mathbb{F}_q^*$ by Lemma 2.7. Then, by Lemma 2.5, we can assume that

$$A_2(2) = q - 2 + \frac{1}{2}(9d - c).$$

Next, we begin to determine the sign of d. By (3.1) and Lemma 3.2, we have

$$A_2(2) = q - 2 + \frac{1}{2}(9d - c) = 9M \equiv 1(\bmod 2).$$

Since

$$q = p^k$$

and a prime

$$p \equiv 1(\bmod 3),$$

we have

$$q \equiv 1(\bmod 2).$$

So, we have

$$-1 + \frac{1}{2}(9d - c) \equiv 1(\bmod 2),$$

and then

$$d \equiv c(\bmod 4).$$

Thus, by Lemma 2.5, we have

$$A_2(4) = q - 2 + \frac{1}{2}(-9d - c).$$

Finally, Theorem 1.2 immediately follows from Lemmas 2.6 and 3.1. □

4. Proof of Theorems 1.3 and an example

Let

$$\mathcal{N}(z) = \{(a_1, a_2, a_3) \in H^3 | a_1 + a_2 + a_3 = z\} \quad \text{and} \quad N(z) = |\mathcal{N}(z)|.$$

Then, if 3 is non-cubic, it is easy to see that

$$27N(z) = A_3(z) - 3A_2(z). \tag{4.1}$$

Lemma 4.1. *If 3 and z are non-cubic in $\mathbb{F}_q^*$, then*

$$A_2(z) = \begin{cases} A_2(3), & \text{if } z \equiv 3(\bmod H), \\ A_2(9), & \text{if } z \equiv 9(\bmod H). \end{cases}$$

Proof. This is similar to the proof of Lemma 3.1. □

Lemma 4.2. *If 3 is non-cubic, we have*

$$N(3) \equiv 1(\bmod 3) \quad \text{and} \quad N(9) \equiv 0(\bmod 3).$$

Proof. We divide the set $\mathcal{N}(z)$ into three disjoint subsets,

$$\mathcal{N}(z) = \mathcal{N}_1(z) \cup \mathcal{N}_2(z) \cup \mathcal{N}_3(z),$$

where

$$\begin{aligned}
\mathcal{N}_1(z) &= \{(a_1, a_2, a_3) \in H^3 | a_1 + a_2 + a_3 = z, a_i \neq a_j, 1 \leq i < j \leq 3\},\\
\mathcal{N}_3(z) &= \{(a, a, a) \in H^3 | a + a + a = z, \},\\
\mathcal{N}_2(z) &= \mathcal{N}(z) \setminus (\mathcal{N}_1(z) \cup \mathcal{N}_3(z)).
\end{aligned}$$

Let

$$N_i(z) = |\mathcal{N}_i(z)|.$$

Then, it is easy to see that

$$N_1(z) \equiv 0 (\bmod 3) \quad \text{and} \quad N_2(z) \equiv 0 (\bmod 3).$$

Since

$$q = p^k$$

and a prime

$$p \equiv 1 (\bmod 3),$$

we have

$$\mathcal{N}_3(3) = \{(1, 1, 1)\}.$$

Thus we have

$$N(3) \equiv 1 (\bmod 3).$$

Since 3 is non-cubic, then

$$\mathcal{N}_3(9) = \emptyset.$$

So, we have

$$N(9) \equiv 0 (\bmod 3).$$

□

Proof of Theorem 1.3. If $3 \mid d$, then 3 is a cube in $\mathbb{F}_q$ by Lemma 2.7, and one has

$$A_2(3) = q - 2 + c \quad \text{and} \quad B_2(3) = q^2 + c(q - 1)$$

as pointed out in [11] (or [12]).

If $3 \nmid d$, then 3 is non-cubic in $\mathbb{F}_q^*$ by Lemma 2.7. Then, by Lemma 2.5, we can assume that

$$A_2(3) = q - 2 + \frac{1}{2}(9d - c),$$

then

$$A_2(9) = q - 2 + \frac{1}{2}(-9d - c).$$

Next, we begin to determine the sign of d.

By (4.1), we have

$$27N(3) = A_3(3) - 3A_2(3), \quad 27N(9) = A_3(9) - 3A_2(9).$$

Then, by Lemma 2.4, we have

$$\begin{aligned}27(N(3) - N(9)) &= A_3(3) - 3A_2(3) - (A_3(9) - 3A_2(9))\\ &= 3A_2(9) - 3A_2(3)\\ &= -27d,\end{aligned}$$

and by Lemma 4.2, we have

$$d = N(9) - N(3) \equiv -1(\text{mod}3).$$

Thus, by Lemma 2.5, we have

$$A_2(3) = q - 2 + \frac{1}{2}(9d - c)$$

with

$$d \equiv -1(\text{mod}3) \quad \text{and} \quad A_2(9) = q - 2 + \frac{1}{2}(-9d - c).$$

Hence, Theorem 1.3 immediately follows from Lemmas 2.6 and 4.1. □

Example 4.3. We take

$$q = 31^2.$$

If the integers c and d satisfy that

$$4 \cdot 31^2 = c^2 + 27d^2, \quad c \equiv 1(\text{mod}3), \quad (c, p) = 1,$$

then

$$c = 46, \quad d = \pm 8.$$

Thus, 2 is cubic and 3 is non-cubic. Then, it follows from Theorem 1.3 that the numbers $A_2(3)$ and $B_2(3)$ of the cubic equations

$$x_1^3 + x_2^3 = 3 \quad \text{and} \quad x_1^3 + x_2^3 + 3x_3^3 = 0$$

are given by

$$A_2(3) = 31^2 - 2 + \frac{1}{2}(9 \cdot 8 - 46) = 972$$

and

$$B_2(3) = 31^4 + \frac{1}{2}(31^2 - 1)(9 \cdot 8 - 46) = 936001,$$

respectively.

5. Conclusions

In this paper, we study the number of solutions of equations:

$$x_1^3 + x_2^3 + zx_3^3 = 0$$

and

$$x_1^3 + x_2^3 = z$$

in finite field $\mathbb{F}_q$ with

$$q = p^k, \quad p \equiv 1(\text{mod}3).$$

When

$$q = p \equiv 1(\text{mod}3),$$

for any z is non-cubic in $\mathbb{F}_p$. In 1978, Chowla et al. determined the sign of d for the case of $z = 2$ being non-cubic in $\mathbb{F}_p$. In Theorem 1.2, we extend the result of Chowla et al. to finite field $\mathbb{F}_q$. In Theorem 1.3, we establish a new method to determine the sign of d for the case of $z = 3$ being non-cubic. Moreover, we think it is interesting to find a more effective way to determine the sign of d for the case of $z > 3$.

Author contributions

Wenxu Ge: writing-review and editing, writing-original draft, validation, resources, methodology, formal analysis, conceptualization. Weiping Li: writing-review and editing, resources, methodology, supervision, validation, formal analysis. Tianze Wang: resources, methodology, supervision, validation, formal analysis, funding acquisition. 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 are partially supported by the National Natural Science Foundation of China (Grant Nos. 11871193 and 12071132), the Natural Science Foundation of Henan Province (Nos. 222300420493 and 232300421223) and the China Scholarship Council (No. 202308410506).

Conflict of interest

The authors declare that they have no conflicts of interest.

References

1. W. X. Ge, W. P. Li, T. Z. Wang, A remark for Gauss sums of order 3 and some applications for cubic congruence equations, *AIMS Math.*, **7** (2022), 10671–10680. https://doi.org/10.3934/math.2022595

2. J. Y. Zhao, On the number of unit solutions of cubic congruence modulo n, *AIMS Math.*, **6** (2021), 13515–13524. https://doi.org/10.3934/math.2021784
3. W. P. Zhang, J. Y. Hu, The number of solutons of the diagonal cubic congruence equation mod$p$, *Math. Rep.*, **20** (2018), 73–80.
4. 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
5. J. Y. Zhao, S. F. Hong, C. X. Zhu, The number of rational points of certain quartic diagonal hypersurfaces over finite fields, *AIMS Math.*, **5** (2020), 2710–2731. https://doi.org/10.3934/math.2020175
6. S. Chowla, J. Cowles, M. Cowles, The number of zeroes of $x^3 + y^3 + cz^3$ in certain finite fields, *J. Reine Angew. Math.*, **299-300** (1978), 406–410. https://doi.org/10.1515/crll.1978.299-300.406
7. S. Chowla, J. Cowles, M. Cowles, Congruence properties of the number of solutions of some equations, *J. Reine Angew. Math.*, **298** (1978), 101–103. https://doi.org/10.1515/crll.1978.298.101
8. S. Chowla, M. Cowles, J. Cowles, On the difference of cubes (mod$p$), *Acta Arith.*, **37** (1980), 61–65.
9. C. F. Gauss, *Disquisitiones arithmeticae*, Yale University, 1966. https://doi.org/10.1007/978-1-4939-7560-0
10. S. Chowla, J. Cowles, M. Cowles, On the number of zeros of diagonal cubic forms, *J. Number Theory*, **9** (1977), 502–506. https://doi.org/10.1016/0022-314X(77)90010-5
11. G. Myerson, On the numbers of zeros of diagonal cubic forms, *J. Number Theory*, **11** (1979), 95–99. https://doi.org/10.1016/0022-314X(79)90023-4
12. S. F. Hong, C. X. Zhu, On the number of zeros of diagonal cubic forms over finite fields, *Forum Math.*, **33** (2021), 697–708. https://doi.org/10.1515/forum-2020-0354
13. G. Myerson, Period polynomials and Gauss sums for finite fields, *Acta Arith.*, **39** (1981), 251–264. https://doi.org/10.4064/AA-39-3-251-264
14. W. X. Ge, W. P. Li, T. Z. Wang, The number of solutions of diagonal cubic equations over finite fields, *Finite Fields Appl.*, **80** (2022), 102008. https://doi.org/10.1016/j.ffa.2022.102008
15. R. Lidl, H. Niederreiter, *Finite fields*, 2 Eds., Cambridge University, 1997. https://doi.org/10.1017/CBO9780511525926
16. B. C. Berndt, K. S. Williams, R. J. Evans, *Gauss Jacobi Sums*, John Wiley & Sons, Inc., 1998.