AIMS Mathematics

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

AIMS Mathematics, 5(3): 2710–2731.
DOI:10.3934/math.2020175
Received: 28 December 2019
Accepted: 10 March 2020
Published: 17 March 2020

Research article

The number of rational points of certain quartic diagonal hypersurfaces over finite fields

Junyong Zhao[1,2], **Shaofang Hong**[1,*] **and Chaoxi Zhu**[1]

[1] Mathematical College, Sichuan University, Chengdu 610064, P. R. China
[2] School of Mathematics and Statistics, Nanyang Institute of Technology, Nanyang 473004, P. R. China

* **Correspondence:** Email: sfhong@scu.edu.cn; Tel: +862885412720; Fax: +862885471501.

Abstract: Let p be an odd prime and let $\mathbb{F}_q$ be a finite field of characteristic p with order $q = p^s$. For $f(x_1, \cdots, x_n) \in \mathbb{F}_q[x_1, ..., x_n]$, we denote by $N(f(x_1, \cdots, x_n) = 0)$ the number of $\mathbb{F}_q$-rational points on the affine hypersurface $f(x_1, \cdots, x_n) = 0$. In 1981, Myerson gave a formula for $N(x_1^4 + \cdots + x_n^4 = 0)$. Recently, Zhao and Zhao obtained an explicit formula for $N(x_1^4 + x_2^4 = c)$ with $c \in \mathbb{F}_q^* := \mathbb{F}_q \setminus \{0\}$. In this paper, by using the Gauss sum and Jacobi sum, we arrive at explicit formulas for $N(x_1^4 + x_2^4 + x_3^4 = c)$ and $N(x_1^4 + x_2^4 + x_3^4 + x_4^4 = c)$ with $c \in \mathbb{F}_q^*$.

Keywords: diagonal hypersurface; rational point; finite field; Gauss sum; Jacobi sum
Mathematics Subject Classification: 11T23, 11T24

1. Introduction

Let $\mathbb{Z}$ and $\mathbb{Z}^+$ stand for the set of all integers and the set of all positive integers. In this paper, we always let p be an odd prime and $\mathbb{F}_q$ be a finite field of $q = p^s$ elements with $s \in \mathbb{Z}^+$. Let $f(x_1, \cdots, x_n)$ be a polynomial with n variables in $\mathbb{F}_q$. We set $N(f = 0)$ to be the number of $\mathbb{F}_q$-rational points of the affine hypersurface $f(x_1, \cdots, x_n) = 0$. That is, one has

$$N(f = 0) = N(f(x_1, \cdots, x_n) = 0) = \sharp\{(x_1, \cdots, x_n) \in \mathbb{F}_q^n | f(x_1, \cdots, x_n) = 0\}.$$

Calculating the exact value of $N(f = 0)$ is a main topic in finite fields. Generally speaking, it is difficult to give an exact formula for $N(f = 0)$. Studying the explicit formula for $N(f = 0)$ under certain conditions has attracted a lot of authors for many years. See, for instance, [1,2,4,6–12,16–24].

In 1977, Chowla, Cowles and Cowles [8] got a formula for the rational points of the hypersurface

$$x_1^3 + x_2^3 + \cdots + x_n^3 = 0$$

in $\mathbb{F}_p$. Recently, Zhang and Hu [23] presented an explicit formula for the rational points of the hypersurface

$$x_1^3 + x_2^3 + x_3^3 + x_4^3 = c,\ c \in \mathbb{F}_p^*.$$

In fact, let $\tilde{N}(c)$ be the rational points of $x_1^3 + x_2^3 + x_3^3 + x_4^3 = c,\ c \in \mathbb{F}_p^*$ with $p \equiv 1 \pmod 3$, and $\mathbb{F}_p^* = \langle g \rangle$ with g being a generator of $\mathbb{F}_p^*$. Then they showed that

$$\tilde{N}(c) = \begin{cases} p^3 - 6p - \frac{1}{2}p(5d \mp 27b), & \text{if } c = g^{3m+1} \text{ with } m \in \mathbb{Z}, \\ p^3 - 6p - \frac{1}{2}p(5d \pm 27b), & \text{if } c = g^{3m+2} \text{ with } m \in \mathbb{Z}, \\ p^3 - 6p + 5dp, & \text{if } c = g^{3m} \text{ with } m \in \mathbb{Z}. \end{cases}$$

On the other hand, Myerson [17] extended the result in [8] to the field $\mathbb{F}_q$ and first studied the rational points of the hypersurface

$$x_1^4 + \cdots + x_n^4 = 0$$

over $\mathbb{F}_q$. Now let $q \equiv 3 \pmod 4$. Then $p \equiv 3 \pmod 4$ and $\gcd(4, q-1) = 2$. Noticing the fact

$$\begin{aligned} N(x_1^4 + \cdots + x_n^4 = c) &= N(x_1^{\gcd(4,q-1)} + \cdots + x_n^{\gcd(4,q-1)} = c) \\ &= N(x_1^2 + \cdots + x_n^2 = c), \end{aligned}$$

it follows from Theorems 6.26 and 6.27 in [15] that the following result is true.

Theorem 1.1. *Let $q \equiv 3 \pmod 4$ and $f(x_1, \cdots, x_n) = x_1^4 + \cdots + x_n^4 - c \in \mathbb{F}_q[x]$ with $c \in \mathbb{F}_q^*$. If n is even, then*

$$N(f = c) = q^{n-1} - q^{\frac{n-2}{2}}\eta((-1)^{\frac{n}{2}}),$$

and if n is odd, then

$$N(f = c) = q^{n-1} + q^{\frac{n-1}{2}}\eta((-1)^{\frac{n-1}{2}}c),$$

where η is the quadratic character of $\mathbb{F}_q$.

By Theorem 1.1, it remains to consider the case $q \equiv 1 \pmod 4$. When $q \equiv 1 \pmod 4$, it is difficult to give an explicit formula for $N(x_1^4 + \cdots + x_n^4 = c)$ with $c \in \mathbb{F}_q^*$ in general. Recently, Zhao and Zhao [24] presented an explicit formula for the number of rational points of the hypersurface $x_1^4 + x_2^4 = c$ with $c \in \mathbb{F}_q^*$.

In this paper, we investigate the number of rational points of the following quartic diagonal hypersurface: $f_1(x_1, x_2, x_3) = c$ and $f_2(x_1, x_2, x_3) = c$, where $c \in \mathbb{F}_q^*$ and

$$f_1(x_1, x_2, x_3) := x_1^4 + x_2^4 + x_3^4$$

and

$$f_2(x_1, x_2, x_3, x_4) := x_1^4 + x_2^4 + x_3^4 + x_4^4.$$

For any primitive element g of $\mathbb{F}_q^*$, we define the *index* of c with respect to g, denoted by $\mathrm{ind}_g(c)$, to be the unique integer $r \in [1, q-1]$ such that $c = g^r$ (see, for instance, [3]). The first main result of this paper can be stated as follows.

Theorem 1.2. *Let $F = \mathbb{F}_q$ be a finite field with $q = p^s$ and $c \in \mathbb{F}_q^*$. Let g be a primitive element of $\mathbb{F}_q^*$.*
(i). *If either $p \equiv 1 \pmod 8$ or $p \equiv 5 \pmod 8$ and s is even, then*

$$N(f_1 = c) = \begin{cases} q^2 + 17q + 6a(-1)^s + 4a^2, & \text{if } \mathrm{ind}_g(c) \equiv 0 \pmod 4, \\ q^2 - 7q + 6a(-1)^s + 4ab, & \text{if } \mathrm{ind}_g(c) \equiv 1 \pmod 4, \\ q^2 - 3q + 6a(-1)^s - 4a^2, & \text{if } \mathrm{ind}_g(c) \equiv 2 \pmod 4, \\ q^2 - 7q + 6a(-1)^s - 4ab, & \text{if } \mathrm{ind}_g(c) \equiv 3 \pmod 4; \end{cases}$$

If $p \equiv 5 \pmod 8$ and s is odd, then

$$N(f_1 = c) = \begin{cases} q^2 - 3q - 6a - 4a^2, & \text{if } \mathrm{ind}_g(c) \equiv 0 \pmod 4, \\ q^2 + 5q - 6a - 4ab, & \text{if } \mathrm{ind}_g(c) \equiv 1 \pmod 4, \\ q^2 - 7q - 6a + 4a^2, & \text{if } \mathrm{ind}_g(c) \equiv 2 \pmod 4, \\ q^2 + 5q - 6a + 4ab, & \text{if } \mathrm{ind}_g(c) \equiv 3 \pmod 4, \end{cases}$$

where $a + b\mathrm{i} = (a' + b'\mathrm{i})^s$ with $\mathrm{i}^2 = -1$ and a' and b' being integers such that

$$a'^2 + b'^2 = p, a' \equiv -1 \pmod 4,\ b' \equiv a' g^{\frac{q-1}{4}} \pmod p.$$

(ii). *Let $p \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$. If $q \equiv 1 \pmod 8$, then*

$$N(f_1 = c) = \begin{cases} q^2 + 17q + 36r^2 + 18r, & \text{if } \mathrm{ind}_g(c) \equiv 0 \pmod 4, \\ q^2 - 7q + 18r \pm 12r\sqrt{q - 9r^2}, & \text{if } \mathrm{ind}_g(c) \equiv 1 \pmod 4, \\ q^2 - 3q - 36r^2 + 18r, & \text{if } \mathrm{ind}_g(c) \equiv 2 \pmod 4, \\ q^2 - 7q + 18r \mp 12r\sqrt{q - 9r^2}, & \text{if } \mathrm{ind}_g(c) \equiv 3 \pmod 4, \end{cases}$$

If $q \equiv 5 \pmod 8$, then

$$N(f_1 = c) = \begin{cases} q^2 + 17q + 36r^2 - 30r + 4, & \text{if } \mathrm{ind}_g(c) \equiv 0 \pmod 4, \\ q^2 - 7q + 18r - 12 \pm 4(3r - 2)\sqrt{q - (3r - 2)^2}, & \text{if } \mathrm{ind}_g(c) \equiv 1 \pmod 4, \\ q^2 - 3q - 36r^2 + 66r - 28, & \text{if } \mathrm{ind}_g(c) \equiv 2 \pmod 4, \\ q^2 - 7q + 18r - 12 \mp 4(3r - 2)\sqrt{q - (3r - 2)^2}, & \text{if } \mathrm{ind}_g(c) \equiv 3 \pmod 4, \end{cases}$$

where r is uniquely determined by $q = r^2 + 4t^2$ with $r \equiv 1 \pmod 4$.

From Theorem 1.1, the following result follows immediately.

Corollary 1.1. *Let $F = \mathbb{F}_q$ be a finite field with $q = p^s$ such that $q \equiv 1 \pmod 4$ and $c \in \mathbb{F}_q^*$. Then $N(f_1 = c) = q^2 + O(q)$.*

Consequently, the second main result of this paper can be stated as follows.

Theorem 1.3. *Let $F = \mathbb{F}_q$ be a finite field with $q = p^s$ and $c \in \mathbb{F}_q^*$. Let g be a primitive element of $\mathbb{F}_q^*$.*

(i). *Let* $p \equiv 1 \pmod 4$. *If* s *is even, then*

$$N(f_2 = c) = \begin{cases} q^3 - (60a + 17)q - 4a^2, & \text{if } \mathrm{ind}_g(c) \equiv 0 \pmod 4, \\ q^3 + (20a - 24b - 17)q - 4a^2, & \text{if } \mathrm{ind}_g(c) \equiv 1 \pmod 4, \\ q^3 + (20a - 17)q - 4a^2, & \text{if } \mathrm{ind}_g(c) \equiv 2 \pmod 4, \\ q^3 + (20a + 24b - 17)q - 4a^2, & \text{if } \mathrm{ind}_g(c) \equiv 3 \pmod 4; \end{cases}$$

If $p \equiv 1 \pmod 8$ *and* s *is odd, then*

$$N(f_2 = c) = \begin{cases} q^3 + (60a - 17)q - 4a^2, & \text{if } \mathrm{ind}_g(c) \equiv 0 \pmod 4, \\ q^3 - (20a - 24b + 17)q - 4a^2, & \text{if } \mathrm{ind}_g(c) \equiv 1 \pmod 4, \\ q^3 - (20a + 17)q - 4a^2, & \text{if } \mathrm{ind}_g(c) \equiv 2 \pmod 4, \\ q^3 - (20a + 24b + 17)q - 4a^2, & \text{if } \mathrm{ind}_g(c) \equiv 3 \pmod 4; \end{cases}$$

If $p \equiv 5 \pmod 8$ *and* s *is odd, then*

$$N(f_2 = c) = \begin{cases} q^3 + (4a + 1)7q - 4a^2, & \text{if } \mathrm{ind}_g(c) \equiv 0 \pmod 4, \\ q^3 - (4a - 8b - 7)q - 4a^2, & \text{if } \mathrm{ind}_g(c) \equiv 1 \pmod 4, \\ q^3 - (20a - 7)q - 4a^2, & \text{if } \mathrm{ind}_g(c) \equiv 2 \pmod 4, \\ q^3 - (4a + 8b - 7)q - 4a^2, & \text{if } \mathrm{ind}_g(c) \equiv 3 \pmod 4 \end{cases}$$

with $a + b\mathrm{i} = (a' + b'\mathrm{i})^s$, *where* a' *and* b' *are integers such that*

$$a'^2 + b'^2 = p,\ a' \equiv -1 \pmod 4,\ b' \equiv a' g^{\frac{q-1}{4}} \pmod p.$$

(ii). *Let* $p \equiv 3 \pmod 4$ *and* $q \equiv 1 \pmod 4$. *If* $q \equiv 1 \pmod 8$, *then*

$$N(f_2 = c) = \begin{cases} q^3 - 17q - 36r^2 - 180rq, & \text{if } \mathrm{ind}_g(c) \equiv 0 \pmod 4, \\ q^2 - 7q + 18r \pm 12r\sqrt{q - 9r^2}, & \text{if } \mathrm{ind}_g(c) \equiv 1 \pmod 4, \\ q^3 - 17q - 36r^2 + 60rq, & \text{if } \mathrm{ind}_g(c) \equiv 2 \pmod 4, \\ q^3 - 17q - 36r^2 + 60rq \pm 24q\sqrt{q - 9r^2}, & \text{if } \mathrm{ind}_g(c) \equiv 3 \pmod 4, \end{cases}$$

If $q \equiv 5 \pmod 8$, *then*

$$N(f_2 = c) = \begin{cases} q^3 + 103q - (6r - 4)^2 - 180rq, & \text{if } \mathrm{ind}_g(c) \equiv 0 \pmod 4, \\ q^3 - 57q - (6r - 4)^2 + 60rq \mp 24q\sqrt{q - (3r - 2)^2}, & \text{if } \mathrm{ind}_g(c) \equiv 1 \pmod 4, \\ q^3 - 57q - (6r - 4)^2 + 60rq, & \text{if } \mathrm{ind}_g(c) \equiv 2 \pmod 4, \\ q^3 - 57q - (6r - 4)^2 + 60rq \pm 24q\sqrt{q - (3r - 2)^2}, & \text{if } \mathrm{ind}_g(c) \equiv 3 \pmod 4, \end{cases}$$

where r *is uniquely determined by* $q = r^2 + 4t^2$ *with* $r \equiv 1 \pmod 4$.

From Theorem 1.2, one can easily deduce the following result.

Corollary 1.2. *Let* $F = \mathbb{F}_q$ *be a finite field with* $q = p^s$ *such that* $q \equiv 1 \pmod 4$ *and* $c \in \mathbb{F}_q^*$. *Then* $N(f_2 = c) = q^3 + O(q^{\frac{3}{2}})$.

This paper is organized as follows. First of all, in Section 2, we present several basic concepts including the Gauss sums and Jacobi sums, and give some preliminary lemmas. Then in Section 3, we give the proofs of Theorems 1.1 and 1.2. Finally, in Section 4, we supply some examples to illustrate the validity of our main results.

2. Preliminary lemmas

In this section, we present several auxiliary lemmas that are needed in the proofs of Theorems 1.1 and 1.2.

Let α be an element of $\mathbb{F}_q$. Then the *trace* and *norm* of α relative to $\mathbb{F}_p$ are defined by (see, for example, [13–15])

$$\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) := \alpha + \alpha^p + \cdots + \alpha^{p^{s-1}}$$

and

$$\mathbb{N}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha) := \alpha\alpha^p \cdots \alpha^{p^{s-1}} = \alpha^{\frac{q-1}{p-1}},$$

respectively. For the simplicity, we write $\mathrm{Tr}(\alpha)$ and $\mathbb{N}(\alpha)$ for $\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)$ and $\mathbb{N}_{\mathbb{F}_q/\mathbb{F}_p}(\alpha)$, respectively. Let χ be a multiplicative character of $\mathbb{F}_q$ and ψ an additive character of $\mathbb{F}_q$. Then we define the *Gauss sum* $G(\chi, \psi)$ by

$$G(\chi, \psi) := \sum_{x \in \mathbb{F}_q^*} \chi(x)\psi(x).$$

Let χ_1 and χ_2 be multiplicative characters of $\mathbb{F}_q$. Then the sum

$$J(\chi_1, \chi_2) := \sum_{x \in \mathbb{F}_q^*} \chi_1(x)\chi_2(1-x)$$

is called a *Jacobi sum* in $\mathbb{F}_q$. The readers are referred to [5] for the basic facts on Jacobi sum.

The character ψ_0 represents the trivial additive character such that $\psi_0(x) = 1$ for all $x \in \mathbb{F}_q$ and χ_0 represents the trivial multiplicative character such that $\chi_0(x) = 1$ for all $x \in \mathbb{F}_q$. For any $x \in \mathbb{F}_q$, let

$$\psi_1(x) := \exp\left(\frac{2\pi i \,\mathrm{Tr}(x)}{p}\right).$$

Then we call ψ_1 the *canonical additive character* of $\mathbb{F}_q$. Let $a \in \mathbb{F}_q$. Then we define

$$\psi_a(x) := \exp\left(\frac{2\pi i \,\mathrm{Tr}(ax)}{p}\right)$$

for all $x \in \mathbb{F}_q$. For each character ψ of $\mathbb{F}_q$ there is associated the conjugate character $\overline{\psi}$ defined by $\overline{\psi}(x) = \overline{\psi(x)}$ for all $x \in \mathbb{F}_q$.

We give several basic identities about Gauss sums as follows.

Lemma 2.1. *[13, 15] Each of the following is true:*

(i). $G(\chi, \psi_{ab}) = \overline{\chi(a)}G(\chi, \psi_b)$ *for* $a \in \mathbb{F}_q^*$, $b \in \mathbb{F}_q$.

(ii). $G(\overline{\chi}, \psi) = \chi(-1)\overline{G(\chi, \psi)}$.

(iii). $|G(\chi, \psi)| = \sqrt{q}$ *for* $\chi \neq \chi_0$ *and* $\psi \neq \psi_0$.

Lemma 2.2. *[13, 15] Let $\mathbb{F}_q$ be a finite field with $q = p^s$ and η be the quadratic character of $\mathbb{F}_q$. Then*

$$G(\eta, \psi_1) = \begin{cases} (-1)^{s-1}\sqrt{q}, & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{s-1}\mathrm{i}^s\sqrt{q}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

If χ_1 and χ_2 are nontrivial, there exists an important connection between Jacobi sums and Gauss sums that will allow us to determine the value of Jacobi sums.

Lemma 2.3. *[13, 15] If χ_1 and χ_2 are multiplicative characters of $\mathbb{F}_q$ and ψ is a nontrivial additive character of $\mathbb{F}_q$, then*

$$J(\chi_1,\chi_2) = \frac{G(\chi_1,\psi)G(\chi_2,\psi)}{G(\chi_1\chi_2,\psi)}$$

if $\chi_1\chi_2$ is nontrivial.

Lemma 2.4. *Let χ be a multiplicative character of $\mathbb{F}_q$ of order n. Then $\chi(-1) = -1$ if and only if n is even and $\frac{q-1}{n}$ is odd.*

Proof. Let g be a generator of $\mathbb{F}_q^*$. Then $g^{q-1} = 1$ and $g^{\frac{q-1}{2}} = -1$.

First, we prove the necessity. Let $\chi(-1) = -1$. For any $x \in \mathbb{F}_q^*$, we have $\chi^{q-1}(x) = \chi(x^{q-1}) = \chi(1) = 1$. Thus $\chi^{q-1} = \chi_0$. Since $\mathrm{ord}(\chi) = n$ and $\chi^{q-1} = \chi_0$, we obtain that $n|(q-1)$. From $(\chi(-1))^n = \chi^n(-1) = \chi_0(-1) = 1$ and $\chi(-1) = -1$, one can deduce that $(-1)^n = 1$. Hence n must be even.

On the other hand, since $g^{\frac{q-1}{2}} = -1$, we have $\chi^{\frac{n}{2}}(g) = \pm 1$. But $\mathrm{ord}(\chi^{\frac{n}{2}}) = 2$ together with the assumption that g is a generator of $\mathbb{F}_q^*$ implies that $\chi^{\frac{n}{2}}(g) \neq 1$. Thus

$$-1 = \chi(-1) = \chi(g^{\frac{q-1}{2}}) = \chi(g^{\frac{n}{2}\frac{q-1}{n}}) = (\chi^{\frac{n}{2}}(g))^{\frac{q-1}{n}} = (-1)^{\frac{q-1}{n}}.$$

Therefore $\frac{q-1}{n}$ is odd as required. The necessity is proved.

Now we prove the sufficiency. Let n be even and $\frac{q-1}{n}$ be odd. Then $\xi := \chi(g)$ is an nth primitive root of unity. Since n is even and $\mathrm{ord}(\xi) = n$, we have $\xi^{\frac{n}{2}} = -1$. Since $\frac{q-1}{n}$ is odd, i.e., $\frac{q-1}{n} \equiv 1 \pmod 2$, one derives that $\frac{q-1}{2} \equiv \frac{n}{2} \pmod n$. Thus

$$\chi(-1) = \chi(g^{\frac{q-1}{2}}) = \xi^{\frac{q-1}{2}} = \xi^{\frac{n}{2}} = -1$$

as desired. Hence the sufficiency part is proved.

This finishes the proof of Lemma 2.4. □

If $p \equiv 3 \pmod 4$, then we easily have the following facts.

$$q = p^s \equiv \begin{cases} 1 \pmod 4, & \text{if and only if } s \text{ is even,} \\ 3 \pmod 4, & \text{if and only if } s \text{ is odd.} \end{cases}$$

If $p \equiv 3 \pmod 4$ and $q = p^s \equiv 3 \pmod 4$, then there does not exist a multiplicative character φ of $\mathbb{F}_q^*$ with $\mathrm{ord}(\varphi) = 4$. Otherwise, if $\varphi \in \widehat{\mathbb{F}_q^*}$ with $\mathrm{ord}(\varphi) = 4$, where $\widehat{\mathbb{F}_q^*}$ is the dual group consisting of all multiplicative characters of $\mathbb{F}_q^*$. Since $\widehat{\mathbb{F}_q^*} \cong \mathbb{F}_q^*$, one has $4 \mid (q-1)$ which is a contradiction.

From the above statement, we deduce the following consequence.

Corollary 2.1. *Let φ be a multiplicative character of $\mathbb{F}_q$ of order 4 with $q = p^s$. Then the following is true.*

(i). *If $p \equiv 1 \pmod 4$, then*

$$\varphi(-1) = \begin{cases} 1, & \text{if } p \equiv 1 \pmod 8 \text{ or } p \equiv 5 \pmod 8 \text{ and } s \text{ is even,} \\ -1, & \text{if } p \equiv 5 \pmod 8 \text{ and } s \text{ is odd.} \end{cases}$$

(ii). *If $p \equiv 3 \pmod 4$, then s is even and $\varphi(-1) = 1$.*

Proof. (i). Since $p \equiv 1 \pmod 4$, we have either $p \equiv 1 \pmod 8$ or $p \equiv 5 \pmod 8$.

If $p \equiv 1 \pmod 8$, then $p^s \equiv 1 \pmod 8$. Hence $\frac{q-1}{4} \equiv 0 \pmod 2$. By Lemma 2.4, we have $\varphi(-1) = 1$.

If $p \equiv 5 \pmod 8$ and s is even, then $p^s \equiv 1 \pmod 8$. Therefore

$$\frac{q-1}{4} = \frac{p^s - 1}{4} \equiv 0 \pmod 2.$$

Then Lemma 2.4 tells us that $\varphi(-1) = 1$.

If $p \equiv 5 \pmod 8$ and s is odd, then $p^s \equiv 5 \pmod 8$. It follows that

$$\frac{q-1}{4} = \frac{p^s - 1}{4} \equiv 1 \pmod 2.$$

So by Lemma 2.4, one can deduce that $\varphi(-1) = -1$. This finishes the proof of (i).

(ii). From the above discussion, we can easily deduce that s is even.

Let $p \equiv 3 \pmod 4$. It implies $p \equiv 3 \pmod 8$ or $p \equiv 5 \pmod 8$. Since s is even, one has $q = p^s \equiv 1 \pmod 8$. It follows that

$$\frac{q-1}{4} = \frac{p^s - 1}{4} \equiv 0 \pmod 2.$$

By Lemma 2.4, one has $\varphi(-1) = 1$. The proof of (ii) is finished. □

Let φ be a generator of $\widehat{\mathbb{F}_q^*}$. Then $\mathrm{ord}(\varphi) = q - 1$ and the multiplicative character λ with order d with $d|(q-1)$ has the expression $\lambda = \varphi^{\frac{q-1}{d}t'}$, where $0 \le t' < d$ and $\gcd(t', d) = 1$. Actually, we have $\lambda = \varphi^t$ with $0 \le t < q - 1$. Hence $\mathrm{ord}(\lambda) = \frac{q-1}{\gcd(t,q-1)}$. Since $\mathrm{ord}(\lambda) = d$, one has $d = \frac{q-1}{\gcd(t,q-1)}$. This infers that $\gcd(t, q-1) = \frac{q-1}{d}$, and so $\frac{q-1}{d} \mid t$. Thus one can write $t = \frac{q-1}{d}t'$ with $1 \le t' \le d$ and $\gcd(t', d) = 1$. That is, one has $\lambda = \varphi^{\frac{q-1}{d}t'}$ with $1 \le t' \le d$ and $\gcd(t', d) = 1$. Moreover, the number of multiplicative character λ with order d is $\phi(d)$, where ϕ is Euler's totient function. In the following, we express the number of solutions of $f(x) = b$ as certain character sums.

Lemma 2.5. *We have*

$$N(x^n = b) = \sum_{j=0}^{\gcd(n,q-1)-1} \lambda^j(b),$$

where λ is a multiplicative character of $\mathbb{F}_q^*$ with order $\gcd(n, q-1)$.

Proof. We divide this into the following three cases. Let λ be any multiplicative character of $\mathbb{F}_q$ with order $d := \gcd(n, q-1)$.

Case 1. $b = 0$. Then $x^n = 0$ has only zero solution $x = 0$ in $\mathbb{F}_q$. That is, one has $N(x^n = 0) = 1$. Since $\lambda^0(0) = 1$ and $\lambda^j(0) = 0$ for $1 \le j \le d-1$, it follows that

$$\sum_{j=0}^{d-1} \lambda^j(0) = 1 = N(x^n = 0)$$

as desired. So part (i) is proved in this case.

Case 2. $b \neq 0$ and $x^n = b$ has a solution in $\mathbb{F}_q$. Let $b = g^k$ and $x = g^y$. Then $x^n = b$ is equivalent to the congruence

$$ny \equiv k \pmod{q-1}. \tag{2.1}$$

Then the congruence (2.1) has exactly $d = \gcd(n, q-1)$ solutions y. Hence $x^n = b$ has exactly d solutions in $\mathbb{F}_q$. Namely, $N(x^n = b) = d$.

Let x_0 be an element of $\mathbb{F}_q$ with $x_0^n = b$. For any integer j with $0 \le j \le d-1$, since $d|n$ implying that $\lambda^n = \chi_0$, the trivial multiplicative character, we have

$$\lambda^j(b) = \lambda^j(x_0^n) = (\lambda^n(x_0))^j = 1.$$

Therefore one derives that

$$\sum_{j=0}^{d-1} \lambda^j(b) = \sum_{j=0}^{d-1} 1 = d = N(x^n = b)$$

as desired. Hence part (i) holds in this case.

Case 3. $b \neq 0$ and $x^n = b$ has no solution in $\mathbb{F}_q$. Then $N(x^n = b) = 0$ and (2.1) has no solution in $\mathbb{F}_q$. Let $b = g^k$. Then $d \nmid k$ and $\lambda(b) = \lambda^k(g) \neq 1$ since $\lambda(g)$ is a d-th primitive root of unity. Then

$$\lambda(b) \sum_{j=0}^{d-1} \lambda^j(b) = \sum_{j=0}^{d-1} \lambda^{j+1}(b) = \sum_{j=0}^{d-1} \lambda^j(b),$$

which implies that

$$(\lambda(b) - 1) \sum_{j=0}^{d-1} \lambda^j(b) = 0.$$

Since $\lambda(b) \neq 1$, we have

$$\sum_{j=0}^{d-1} \lambda^j(b) = 0 = N(x^n = b)$$

as required.

The proof of Lemma 2.5 is complete. □

Let χ' be a multiplicative character of $\mathbb{F}_p$ and ψ' be an additive character of $\mathbb{F}_p$. From the multiplicativity of the norm and the additivity of the trace, it follows that $\chi' \circ \mathbb{N}$ is a multiplicative and $\psi' \circ \mathrm{Tr}$ an additive character of $\mathbb{F}_q$. We say that the multiplicative character χ of $\mathbb{F}_q$ is lifted from the multiplicative character χ' of $\mathbb{F}_p$ if $\chi = \chi' \circ \mathbb{N}$. We also say that the multiplicative character χ' of $\mathbb{F}_p$ is lifting to the multiplicative character χ of $\mathbb{F}_q$. Similarly, we say that the additive character ψ of $\mathbb{F}_q$ is lifted from the additive character ψ' of $\mathbb{F}_p$ if $\psi = \psi' \circ \mathrm{Tr}$. We also say that the additive character ψ' of $\mathbb{F}_p$ is lifting to the additive character ψ of $\mathbb{F}_q$. The following lemma is due to Hasse and Davenport establishes an important relationship between the Gauss sum $G(\chi', \psi')$ of $\mathbb{F}_p$ and the Gauss sum $G(\chi, \psi)$ of $\mathbb{F}_q$.

Lemma 2.6. *[13, 15] Let ψ' be an additive and χ' a multiplicative character of $\mathbb{F}_p$, not both of them trivial. Suppose that ψ' and χ' are lifting to characters ψ and χ, respectively, of the finite extension field $\mathbb{F}_q$ of $\mathbb{F}_p$ with $[\mathbb{F}_q : \mathbb{F}_p] = s$. Then*

$$G(\chi, \psi) = (-1)^{s-1} G^s(\chi', \psi').$$

The characters of $\mathbb{F}_p$ can be lifted to the characters of $\mathbb{F}_q$, but not all the characters of $\mathbb{F}_q$ can be obtained by lifting a character of $\mathbb{F}_p$. The following result characterizes all the characters of $\mathbb{F}_q$ that can be obtained by lifting a character of $\mathbb{F}_p$.

Lemma 2.7. *Let χ be a multiplicative character of $\mathbb{F}_q$ with $q = p^s$. Then χ can be lifted from a multiplicative character χ' of $\mathbb{F}_p$ if and only if χ^{p-1} is trivial.*

Proof. Let g be a generator of $\mathbb{F}_q^*$. Since

$$\mathbb{N}^{p-1}(g) = (g^{\frac{q-1}{p-1}})^{p-1} = g^{q-1} = 1$$

and

$$\mathbb{N}^l(g) = (g^{\frac{q-1}{p-1}})^l \neq 1 \text{ for } 1 \leq l < p-1,$$

one knows that $\mathbb{N}(g)$ is a generator of $\mathbb{F}_p^*$.

First of all, we prove the necessity. Suppose that χ can be obtained by lifting a multiplicative character χ' of $\mathbb{F}_p$. It then follows that $\chi(g) = \chi'(\mathbb{N}(g))$. Since χ' is a character of $\mathbb{F}_p^*$, we get that the values of χ' are $(p-1)$-th roots of unity. Hence

$$\chi^{p-1}(g) = \chi'^{p-1}(\mathbb{N}(g)) = \big(\chi'(\mathbb{N}(g))\big)^{p-1} = 1.$$

Thus χ^{p-1} is trivial. The necessity is proved.

Now we prove the sufficiency. Let χ^{p-1} be trivial. Since χ is a multiplicative character of $\mathbb{F}_q^*$, $\chi(g)$ must be a $(q-1)$-th roots of unity, say

$$\chi(g) := \exp\Big(\frac{2\pi \mathrm{i} j}{q-1}\Big) \tag{2.2}$$

for some integer j with $0 \leq j \leq q-2$, where throughout this paper, i stands for the 4-th primitive root of unity, i.e. $\mathrm{i}^4 = 1$ and $\mathrm{i}^2 \neq 1$. Since χ^{p-1} is trivial, we have

$$\chi^{p-1}(g) = \exp\Big(\frac{2\pi \mathrm{i} j(p-1)}{q-1}\Big) = 1.$$

This implies that $(q-1) \mid j(p-1)$. It follows that $\frac{q-1}{p-1} \mid j$. Therefore we derive that

$$j = k\frac{q-1}{p-1}$$

for some $k \in \mathbb{Z}$.

By substituting $j = k\frac{q-1}{p-1}$ in (2.2), we obtain that

$$\chi(g) = \exp\Big(\frac{2\pi \mathrm{i} k}{p-1}\Big). \tag{2.3}$$

Since $\mathbb{N}(g)$ is a generator of $\mathbb{F}_p^*$, one can define a multiplicative character χ' of $\mathbb{F}_p^*$ by

$$\chi'(\mathbb{N}(g)) := \exp\Big(\frac{2\pi \mathrm{i} k}{p-1}\Big). \tag{2.4}$$

From (2.3) and (2.4), we get $\chi(g) = \chi'(\mathbb{N}(g))$. This completes the sufficiency.

This finishes the proof of Lemma 2.7. □

For a certain special multiplicative character of $\mathbb{F}_p$, the following result gives an explicit formula about the associated Jacobi sums.

Lemma 2.8. *[5] Let $p \equiv 1 \pmod 4$ be an odd prime number and let φ' be a multiplicative character of $\mathbb{F}_p$ with ord$(\varphi') = 4$. If θ is a generator of $\mathbb{F}_p^*$ with $\varphi'(\theta) = \mathrm{i}$, then*

$$J(\varphi', \varphi') = a' + b'\mathrm{i},$$

where a' and b' are integers such that $a'^2 + b'^2 = p$, $a' \equiv -1 \pmod 4$ and $b' \equiv a'\theta^{\frac{p-1}{4}} \pmod p$.

For a certain special multiplicative character of $\mathbb{F}_q$, we establish an explicit formula of the associated Gauss sums.

Lemma 2.9. *Let $\mathbb{F}_q$ be a finite field with $q = p^s$, where $p \equiv 1 \pmod 4$ is an odd prime and $s \in \mathbb{Z}^+$. Let φ be a multiplicative character of $\mathbb{F}_q$ with* ord$(\varphi) = 4$ *and g be a primitive element of $\mathbb{F}_q^*$ with $\varphi(g) = \mathrm{i}$. Then*

$$G^2(\varphi, \psi_1) = (a' + b'\mathrm{i})^s \sqrt{q},$$

where a' and b' are integers such that

$$a'^2 + b'^2 = p, \quad a' \equiv -1 \pmod 4, \quad b' \equiv a' g^{\frac{q-1}{4}} \pmod p.$$

Proof. First we claim that if $\chi = \chi' \circ \mathbb{N}$, then ord$(\chi)$ = ord(χ'). To prove it, we let ord$(\chi') = m$ and ord$(\chi) = l$. Since $\mathbb{N}(x) \in \mathbb{F}_p^*$ for all $x \in \mathbb{F}_q^*$, we have

$$\chi^m(x) = (\chi'(\mathbb{N}(x)))^m = \chi'^m(\mathbb{N}(x)) = \chi_0(\mathbb{N}(x)) = 1.$$

It follows that $l|m$. Conversely, let g' be a generator of $\mathbb{F}_p^*$. Then $\chi'(g')$ is a primitive m-th root of unity. Since the norm map $\mathbb{N}$ is surjective, there exist an element $g \in \mathbb{F}_q^*$ such that $\mathbb{N}(g) = g'$. Then we have

$$1 = \chi^l(g) = (\chi'(\mathbb{N}(g)))^l = \chi'^l(\mathbb{N}(g)) = \chi'^l(g')$$

Hence one can deduce that $m|l$. So the desired result $l = m$ follows immediately. Namely, we have ord(χ) = ord(χ'). The claim is proved.

Since ord$(\varphi) = 4$ and $p \equiv 1 \pmod 4$, we derive that φ^{p-1} is trivial. By Lemma 2.7, φ can be obtained by lifting a character φ' of $\mathbb{F}_p^*$. Morever, the additive character $\psi_1'(x) = \exp\left(\frac{2\pi\mathrm{i}x}{p}\right)$ of $\mathbb{F}_p$ can be lifted to the additive character $\psi_1(x) = \exp\left(\frac{2\pi\mathrm{i}\,\mathrm{Tr}(x)}{p}\right)$ of $\mathbb{F}_q$. By the famous Hasse-Davenport relation (see Lemma 2.6), we get that

$$G(\varphi, \psi_1) = (-1)^{s-1} G^s(\varphi', \psi_1').$$

Hence

$$G^2(\varphi, \psi_1) = (G^2(\varphi', \psi_1'))^s. \tag{2.5}$$

By Lemma 2.3, the following identity is true:

$$G^2(\varphi', \psi_1') = J(\varphi', \varphi') G((\varphi')^2, \psi_1'). \tag{2.6}$$

Since ord$(\varphi') = 4$, one has ord$((\varphi')^2) = 2$. Then by Lemma 2.2, we have

$$G((\varphi')^2, \psi_1') = \sqrt{p}. \tag{2.7}$$

Now we evaluate $J(\varphi', \varphi')$. Since the order of lifting character is invariant, we have $\mathrm{ord}(\varphi') = \mathrm{ord}(\varphi) = 4$. Note that $\mathrm{ord}(\mathbb{N}(g)) = p - 1$. It means that $\mathbb{N}(g)$ is a primitive element of $\mathbb{F}_p^*$. Noticing that $\mathrm{i} = \varphi(g) = \varphi'(\mathbb{N}(g)))$ and $\mathrm{ord}(\varphi') = 4$, Lemma 2.8 tells that

$$J(\varphi', \varphi') = a' + b'\mathrm{i},$$

where a' and b' are integers such that

$$a'^2 + b'^2 = p, \quad a' \equiv -1 \pmod 4, \quad b' \equiv a'\mathbb{N}(g)^{\frac{p-1}{4}} \pmod p. \tag{2.8}$$

But $\mathbb{N}(g) = g^{\frac{q-1}{p-1}}$. It then follows from (2.8) that

$$b' \equiv a' g^{\frac{q-1}{4}} \pmod p. \tag{2.9}$$

From (2.6) to (2.9), we deduce that

$$G^2(\varphi', \psi_1') = (a' + b'\mathrm{i})\sqrt{p}. \tag{2.10}$$

It follows from (2.7), (2.10) and $q = p^s$ that

$$G^2(\varphi, \psi_1) = (a' + b'\mathrm{i})^s \sqrt{q},$$

where a' and b' are integers satisfying (2.8).

This concludes the proof of Lemma 2.9. □

Lemma 2.10. *Let $\mathbb{F}_q$ be a finite field with $q = p^s$ elements and $q \equiv 1 \pmod 4$. Let φ be a multiplicative character of $\mathbb{F}_q^*$ with $\mathrm{ord}(\varphi) = 4$ and $c \in \mathbb{F}_q^*$. Then we have*

$$\begin{aligned} &N(x_1^4 + ... + x_n^4 = c) \\ =&q^{n-1} + \frac{1}{q}\sum_{x\in\mathbb{F}_q^*}\Big(\overline{\varphi}(x)G(\varphi, \psi_1) + \Big(\frac{\mathbb{N}(x)}{p}\Big)(-1)^{s-1}\sqrt{q} + \varphi(-x)\overline{G(\varphi, \psi_1)}\Big)^n \psi_1(-xc). \end{aligned}$$

Proof. For $x \in \mathbb{F}_q$, from the trigonometric identity

$$\sum_{y\in\mathbb{F}_q} \exp\Big(\frac{2\pi\mathrm{i}\,\mathrm{Tr}(xy)}{p}\Big) = \begin{cases} q, & \text{if } x = 0, \\ 0, & \text{if } x \neq 0, \end{cases}$$

we can deduce that

$$\begin{aligned} N(x_1^4 + ... + x_n^4 = c) &= \frac{1}{q}\sum_{x\in\mathbb{F}_q}\sum_{(x_1,...,x_n)\in\mathbb{F}_q^n} \exp\Big(\frac{2\pi\mathrm{i}\,\mathrm{Tr}(x(x_1^4 + ... + x_n^4 - c))}{p}\Big) \\ &= \frac{1}{q}\sum_{x\in\mathbb{F}_q}\Big(\sum_{y\in\mathbb{F}_q}\exp\Big(\frac{2\pi\mathrm{i}\,\mathrm{Tr}(xy^4)}{p}\Big)\Big)^n \exp\Big(\frac{2\pi\mathrm{i}\,\mathrm{Tr}(-xc)}{p}\Big) \\ &= q^{n-1} + \frac{1}{q}\sum_{x\in\mathbb{F}_q^*}\Big(\sum_{y\in\mathbb{F}_q}\exp\Big(\frac{2\pi\mathrm{i}\,\mathrm{Tr}(xy^4)}{p}\Big)\Big)^n \psi_1(-xc). \end{aligned} \tag{2.11}$$

Denote

$$R_x := \sum_{y\in\mathbb{F}_q} \exp\Big(\frac{2\pi \mathrm{i}\,\mathrm{Tr}(xy^4)}{p}\Big).$$

By Lemma 2.5, we get that

$$\begin{aligned} R_x &= 1 + \sum_{z\in\mathbb{F}_q^*} N(y^4 = z) \exp\Big(\frac{2\pi \mathrm{i}\,\mathrm{Tr}(xz)}{p}\Big) \\ &= 1 + \sum_{z\in\mathbb{F}_q^*} \Big(1 + \varphi(z) + \varphi^2(z) + \varphi^3(z)\Big) \exp\Big(\frac{2\pi \mathrm{i}\,\mathrm{Tr}(xz)}{p}\Big) \\ &= 1 + \sum_{z\in\mathbb{F}_q^*} \Big(1 + \varphi(z) + \varphi^2(z) + \varphi^3(z)\Big)\psi_1(xz), \end{aligned}$$

where φ is a multiplicative character of $\mathbb{F}_q$ with $\mathrm{ord}(\varphi) = 4$. Then $\varphi(g) = \pm\mathrm{i}$. WLOG, in what follows, we set $\varphi(g) = \mathrm{i}$.

Note that $\varphi^2 = \eta$ and $\varphi^3 = \overline{\varphi}$, we know that

$$R_x = \sum_{z\in\mathbb{F}_q} \psi_1(xz) + \sum_{z\in\mathbb{F}_q^*} \varphi(z)\psi_1(xz) + \sum_{z\in\mathbb{F}_q^*} \eta(z)\psi_1(xz) + \sum_{z\in\mathbb{F}_q^*} \overline{\varphi}(z)\psi_1(xz).$$

Since

$$\sum_{z\in\mathbb{F}_q} \psi_1(xz) = 0,$$

it follows from the definition of Gauss sum and Lemma 2.1 that

$$\begin{aligned} R_x &= \sum_{z\in\mathbb{F}_q^*} \varphi(z)\psi_1(xz) + \sum_{z\in\mathbb{F}_q^*} \eta(z)\psi_1(xz) + \sum_{z\in\mathbb{F}_q^*} \overline{\varphi}(z)\psi_1(xz) \\ &= G(\varphi, \psi_x) + G(\eta, \psi_x) + G(\overline{\varphi}, \psi_x) \\ &= \overline{\varphi}(x)G(\varphi, \psi_1) + \overline{\eta}(x)G(\eta, \psi_1) + \varphi(x)G(\overline{\varphi}, \psi_1). \end{aligned}$$

Note that the value of η is real and $\eta(x) = \Big(\frac{\mathbb{N}(x)}{p}\Big)$, from the Lemmas 2.1 and 2.2 we deduce that

$$R_x = \overline{\varphi}(x)G(\varphi, \psi_1) + \Big(\frac{\mathbb{N}(x)}{p}\Big)(-1)^{s-1}\sqrt{q} + \varphi(-x)\overline{G(\varphi, \psi_1)}. \tag{2.12}$$

So the desired result follows immediately. □

Lemma 2.11. *Let $\mathbb{F}_q$ be a finite field of $q = p^s$ with $p \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$. Let φ be a multiplicative character of $\mathbb{F}_q^*$ with ord$(\varphi) = 4$. Then*

$$G^2(\varphi, \psi_1) + \overline{G^2(\varphi, \psi_1)} = \begin{cases} 6r\sqrt{q}, & \text{if } q \equiv 1 \pmod 8, \\ (6r-4)\sqrt{q}, & \text{if } q \equiv 5 \pmod 8, \end{cases}$$

where r is uniquely determined by

$$q = r^2 + 4t^2,\ r \equiv 1 \pmod 4.$$

Proof. By $p \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$, we can deduce s is even immediately.

First of all, we calculate $N(x_1^4 + x_2^4 = -1)$ using Lemma 2.10. Setting $n = 2$ in Lemma 2.10 gives us that

$$\begin{aligned} &N(x_1^4 + x_2^4 = c) \\ =&q + \frac{1}{q}\sum_{x\in\mathbb{F}_q^*}\Big(\overline{\varphi}(x)G(\varphi,\psi_1) + \Big(\frac{\mathbb{N}(x)}{p}\Big)(-1)^{s-1}\sqrt{q} + \varphi(-x)\overline{G(\varphi,\psi_1)}\Big)^2\psi_1(-xc) \\ :=&q + \frac{1}{q}\sum_{x\in\mathbb{F}_q^*}T_x''. \end{aligned} \tag{2.13}$$

Since $\varphi^3 = \overline{\varphi}$, $\overline{\varphi^2} = \varphi^2 = \eta$, $\varphi^2(x) = \Big(\frac{\mathbb{N}(x)}{p}\Big)$ and Lemma 2.1 implying that

$$G(\varphi,\psi_1)\overline{G(\varphi,\psi_1)} = q,$$

it follows that

$$\begin{aligned} T_x'' =&\Big(\eta(x)(G^2(\varphi,\psi_1) + \overline{G^2(\varphi,\psi_1)}) + 2(-1)^{s-1}\sqrt{q}(\varphi(x)G(\varphi,\psi_1) + \varphi(-1)\overline{\varphi}(x)\overline{G(\varphi,\psi_1)}) \\ &+ (1 + 2\varphi(-1))q\Big)\psi_1(-xc). \end{aligned}$$

By using the following simple facts

$$\eta(x) = \frac{\eta(-xc)}{\eta(-c)}, \quad \varphi(x) = \frac{\varphi(-1)}{\varphi(c)}\varphi(-xc), \quad \overline{\varphi}(x) = \frac{\varphi(-1)}{\overline{\varphi}(c)}\overline{\varphi}(-xc),$$

we deduce that

$$\begin{aligned} T_x'' =&\Big(\frac{\eta(-xc)}{\eta(-c)}(G^2(\varphi,\psi_1) + \overline{G^2(\varphi,\psi_1)}) + (1 + 2\varphi(-1))q \\ &+ 2(-1)^{s-1}\sqrt{q}\Big(\frac{\varphi(-1)}{\varphi(c)}\varphi(-xc)G(\varphi,\psi_1) + \frac{1}{\overline{\varphi}(c)}\overline{\varphi}(-xc)\overline{G(\varphi,\psi_1)}\Big)\Big)\psi_1(-xc). \end{aligned} \tag{2.14}$$

Since $-xc$ runs over $\mathbb{F}_q^*$ as x runs through $\mathbb{F}_q^*$, it follows from (2.13), (2.14) and the fact of $\sum\limits_{x\in\mathbb{F}_q^*}\psi_1(-xc) = -1$ that

$$\begin{aligned} &N(x_1^4 + x_2^4 = c) \\ &= q + \frac{1}{q}\Big(\frac{G^2(\varphi,\psi_1) + \overline{G^2(\varphi,\psi_1)}}{\eta(-c)}G(\eta,\psi_1) - (1 + 2\varphi(-1))q \\ &+ 2(-1)^{s-1}\sqrt{q}\frac{\varphi(-1)}{\varphi(c)}G^2(\varphi,\psi_1) + (-1)^{s-1}\sqrt{q}\frac{2}{\overline{\varphi}(c)}\overline{G(\varphi,\psi_1)}G(\overline{\varphi},\psi_1)\Big). \end{aligned} \tag{2.15}$$

Since s is even. From Lemma 2.1, 2.2, Corollary 2.1 and (2.15), one has

$$N(x_1^4 + x_2^4 = -1) = q - 3 - \frac{G^2(\varphi,\psi_1) + \overline{G^2(\varphi,\psi_1)}}{\sqrt{q}}. \tag{2.16}$$

Consequently, we calculate $N(x_1^4 + x_2^4 = -1)$ by using another method. Let N_n be the number of solutions of

$$x_1^4 + x_2^4 + \cdots + x_n^4 = 0$$

over $\mathbb{F}_q$. From Lemma 6 to Lemma 8 in [17], we can easily derive that

$$N_2 = \begin{cases} 4q - 3, & \text{if } q \equiv 1 \pmod 8, \\ 1, & \text{if } q \equiv 5 \pmod 8 \end{cases}$$

and

$$N_3 = q^2 - 6rq + 6r,$$

where r is uniquely determined by

$$q = r^2 + 4t^2,\ r \equiv 1 \pmod 4.$$

Since

$$N_3 = \sum_{\substack{(x_1,x_2,x_3)\in\mathbb{F}_q^3 \\ x_1^4+x_2^4+x_3^4=0}} 1 = \sum_{\substack{(x_1,x_2)\in\mathbb{F}_q^2 \\ x_1^4+x_2^4=0}} 1 + \sum_{\substack{x_3\in\mathbb{F}_q^* \\ x_1^4+x_2^4=-x_3^4}} 1$$

$$= N_2 + (q-1)N(x_1^4 + x_2^4 = -1),$$

one has

$$\begin{aligned} N(x_1^4 + x_2^4 = -1) &= \frac{N_3 - N_2}{q-1} \\ &= \begin{cases} \frac{q^2-(6r+4)q+(6r+3)}{q-1}, & \text{if } q \equiv 1 \pmod 8, \\ \frac{q^2-6rq+(6r-1)}{q-1}, & \text{if } q \equiv 5 \pmod 8. \end{cases} \end{aligned} \tag{2.17}$$

From (2.16) and (2.17), one deduces that

$$G^2(\varphi,\psi_1) + \overline{G^2(\varphi,\psi_1)} = \begin{cases} 6r\sqrt{q}, & \text{if } q \equiv 1 \pmod 8, \\ (6r-4)\sqrt{q}, & \text{if } q \equiv 5 \pmod 8 \end{cases}$$

as desired. This completes the proof of Lemma 2.11. □

Remark 2.1. *From Lemma 2.11, we can write*

$$G^2(\varphi,\psi_1) = \begin{cases} 3r\sqrt{q} + A\mathrm{i}, & \textit{if } q \equiv 1 \pmod 8, \\ (3r-2)\sqrt{q} + B\mathrm{i}, & \textit{if } q \equiv 5 \pmod 8. \end{cases}$$

But it is known that $G^2(\varphi,\psi_1)\overline{G^2(\varphi,\psi_1)} = q^2$. *So one has* $A = \pm\sqrt{q^2 - 9r^2q}$ *and* $B = \pm\sqrt{q^2 - (3r-2)^2q}$.

3. Proofs of Theorems 1.2 and 1.3

In this section, we present the proofs of the main results of this paper. We begin with the proof of Theorem 1.2.

Proof of Theorem 1.2. (i). Let $p \equiv 1 \pmod 4$. Then Lemma 2.10 applied to $n = 3$ gives us that

$$\begin{aligned} &N(f_1 = c) \\ &= q^2 + \frac{1}{q}\sum_{x\in\mathbb{F}_q^*}\Big(\overline{\varphi}(x)G(\varphi,\psi_1) + \Big(\frac{\mathbb{N}(x)}{p}\Big)(-1)^{s-1}q^{\frac{1}{2}} + \varphi(-x)\overline{G(\varphi,\psi_1)}\Big)^3\psi_1(-xc) \\ &:= q^2 + \frac{1}{q}\sum_{x\in\mathbb{F}_q^*}T_x. \end{aligned} \tag{3.1}$$

Since $\varphi^3 = \overline{\varphi}$, $\varphi^2(x) = \Big(\frac{\mathbb{N}(x)}{p}\Big)$ and Lemma 2.1 implying that $G(\varphi,\psi_1)\overline{G(\varphi,\psi_1)} = q$, it follows that

$$\begin{aligned} T_x =&(\varphi(x)G^3(\varphi,\psi_1) + \varphi^2(x)(-1)^{s-1}q^{\frac{3}{2}} + \varphi(-1)\overline{\varphi}(x)\overline{G^3(\varphi,\psi_1)} \\ &+ 3(-1)^{s-1}G^2(\varphi,\psi_1)q^{\frac{1}{2}} + 3\varphi(-1)\overline{\varphi}(x)G(\varphi,\psi_1)q + 3\overline{\varphi}(x)G(\varphi,\psi_1)q \\ &+ 3\varphi(x)\overline{G(\varphi,\psi_1)}q + 3\varphi(-1)\varphi(x)\overline{G(\varphi,\psi_1)}q + 3(-1)^{s-1}\overline{G^2(\varphi,\psi_1)}q^{\frac{1}{2}} \\ &+ 6\varphi(-1)(-1)^{s-1}\varphi^2(x)q^{\frac{3}{2}})\psi_1(-xc). \end{aligned}$$

By using the following simple facts

$$\varphi(x) = \frac{\varphi(-1)}{\varphi(c)}\varphi(-xc), \quad \overline{\varphi}(x) = \frac{\varphi(-1)}{\overline{\varphi}(c)}\overline{\varphi}(-xc),$$

we deduce that

$$\begin{aligned} T_x =& \Big(\frac{\varphi(-1)}{\varphi(c)}\varphi(-xc)G^3(\varphi,\psi_1) + \frac{1}{\varphi^2(c)}\varphi^2(-xc)(-1)^{s-1}q^{\frac{3}{2}} + \frac{1}{\overline{\varphi}(c)}\overline{\varphi}(-xc)\overline{G^3(\varphi,\psi_1)} \\ &+ 3(-1)^{s-1}G^2(\varphi,\psi_1)q^{\frac{1}{2}} + \frac{3}{\overline{\varphi}(c)}\overline{\varphi}(-xc)G(\varphi,\psi_1)q + 3\frac{\varphi(-1)}{\overline{\varphi}(c)}\overline{\varphi}(-xc)G(\varphi,\psi_1)q \\ &+ 3\frac{\varphi(-1)}{\varphi(c)}\varphi(-xc)\overline{G(\varphi,\psi_1)}q + \frac{3}{\varphi(c)}\varphi(-xc)\overline{G(\varphi,\psi_1)}q + 3(-1)^{s-1}\overline{G^2(\varphi,\psi_1)}q^{\frac{1}{2}} \\ &+ 6\frac{\varphi(-1)}{\varphi^2(c)}(-1)^{s-1}\varphi^2(-xc)q^{\frac{3}{2}}\Big)\psi_1(-xc). \end{aligned} \tag{3.2}$$

Since $-xc$ runs over $\mathbb{F}_q^*$ as x runs through $\mathbb{F}_q^*$, it follows from (3.1), (3.2) and the definition of Gauss sum that

$$\begin{aligned} &N(f_1 = c) \\ &= q^2 + \frac{1}{q}\Big(\frac{\varphi(-1)}{\varphi(c)}G^4(\varphi,\psi_1) + (-1)^{s-1}q^{\frac{3}{2}}\frac{1}{\varphi^2(c)}G(\varphi^2,\psi_1) \\ &+ \frac{1}{\overline{\varphi}(c)}\overline{G^3(\varphi,\psi_1)}G(\overline{\varphi},\psi_1) + 3(-1)^{s-1}q^{\frac{1}{2}}G^2(\varphi,\psi_1)\sum_{x\in\mathbb{F}_q^*}\psi_1(-xc) \end{aligned}$$

$$+\frac{3q}{\overline{\varphi}(c)}G(\varphi,\psi_1)G(\overline{\varphi},\psi_1)+3q\frac{\varphi(-1)}{\overline{\varphi}(c)}G(\varphi,\psi_1)G(\overline{\varphi},\psi_1)$$
$$+3q\frac{\varphi(-1)}{\varphi(c)}\overline{G(\varphi,\psi_1)}G(\varphi,\psi_1)+\frac{3q}{\varphi(c)}\overline{G(\varphi,\psi_1)}G(\varphi,\psi_1)$$
$$+3(-1)^{s-1}q^{\frac{1}{2}}\overline{G^2(\varphi,\psi_1)}\sum_{x\in\mathbb{F}_q^*}\psi_1(-xc)+6(-1)^{s-1}q^{\frac{3}{2}}\frac{\varphi(-1)}{\varphi^2(c)}G(\varphi^2,\psi_1)\Big).$$

Note that $\frac{1}{\varphi(c)}=\overline{\varphi}(c)$, $\quad\overline{\varphi}^2(c)=\varphi^2(c)$. Then from Lemmas 2.1 and 2.2, we derive that

$$N(f_1=c)=q^2+(6\varphi(-1)+1)\varphi^2(c)q+(1+\varphi(-1))3q(\varphi(c)+\overline{\varphi}(c))$$
$$-3(-1)^{s-1}q^{-\frac{1}{2}}\Big(G^2(\varphi,\psi_1)+\overline{G^2(\varphi,\psi_1)}\Big)+\frac{\varphi(-1)}{q}(\overline{\varphi}(c)G^4(\varphi,\psi_1)+\varphi(c)\overline{G^4(\varphi,\psi_1)}). \tag{3.3}$$

Since $\varphi(1)=\overline{\varphi}(1)=1$, it follows from (3.3) that

$$N(f_1=1)=q^2+(10\varphi(-1)+7)q-3(-1)^{s-1}q^{-\frac{1}{2}}(G^2((\varphi,\psi_1)+\overline{G^2(\varphi,\psi_1)}))$$
$$+\frac{1}{q}\varphi(-1)(G^2((\varphi,\psi_1)+\overline{G^2(\varphi,\psi_1)}))^2.$$

From Lemma 2.9 and letting $a+b\mathrm{i}:=(a'+b'\mathrm{i})^s$, we know that

$$G^2(\varphi,\psi_1)+\overline{G^2(\varphi,\psi_1)}=2a\sqrt{q},\quad G^2(\varphi,\psi_1)-\overline{G^2(\varphi,\psi_1)}=2b\mathrm{i}\sqrt{q}. \tag{3.4}$$

Thus

$$N(f_1=1)=q^2+(10\varphi(-1)+7)q+6a(-1)^s+4a^2\varphi(-1).$$

Then by Corollary 2.1 we get

$$N(f_1=1)=\begin{cases}q^2+17q+6a(-1)^s+4a^2, & \text{if either } p\equiv 1 \pmod 8,\\ & \text{or } p\equiv 5 \pmod 8 \text{ and } s \text{ is even},\\ q^2-3q-6a-4a^2, & \text{if } p\equiv 5 \pmod 8 \text{ and } s \text{ is odd}.\end{cases} \tag{3.5}$$

From (3.3), (3.4) and noticing that $\varphi(g)=\mathrm{i}$, we obtain that

$$N(f_1=g)=q^2-(6\varphi(-1)+1)q+6a(-1)^s+4ab\varphi(-1).$$

So applying Corollary 2.1 gives that

$$N(f_1=g)=\begin{cases}q^2-7q+6a(-1)^s+4ab, & \text{if either } p\equiv 1 \pmod 8,\\ & \text{or } p\equiv 5 \pmod 8 \text{ and } s \text{ is even},\\ q^2+5q-6a-4ab, & \text{if } p\equiv 5 \pmod 8 \text{ and } s \text{ is odd}.\end{cases} \tag{3.6}$$

Similarly, from $\varphi(g^2)=-1$ and $\varphi(g^3)=-\mathrm{i}$, one can deduce that

$$N(f_1=g^2)=\begin{cases}q^2-3q+6a(-1)^s-4a^2, & \text{if either } p\equiv 1 \pmod 8,\\ & \text{or } p\equiv 5 \pmod 8 \text{ and } s \text{ is even},\\ q^2-7q-6a+4a^2, & \text{if } p\equiv 5 \pmod 8 \text{ and } s \text{ is odd}\end{cases} \tag{3.7}$$

and

$$N(f_1 = g^3) = \begin{cases} q^2 - 7q + 6a(-1)^s - 4ab, & \text{if either } p \equiv 1 \pmod 8, \\ & \text{or } p \equiv 5 \pmod 8 \text{ and } s \text{ is even}, \\ q^2 + 5q - 6a + 4ab, & \text{if } p \equiv 5 \pmod 8 \text{ and } s \text{ is odd}. \end{cases} \tag{3.8}$$

Hence part (i) of Theorem 1.2 is proved.

(ii). Let $p \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$. Then s is even. From Corollary 2.1 and (3.3), one has

$$\begin{aligned} N(f_1 = c) &= q^2 + 7q\varphi^2(c) + 6q(\varphi(c) + \overline{\varphi}(c)) \\ &+ 3\frac{G^2(\varphi, \psi_1) + \overline{G^2(\varphi, \psi_1)}}{\sqrt{q}} + \frac{\overline{\varphi}(c)G^4(\varphi, \psi_1) + \varphi(c)\overline{G^4(\varphi, \psi_1)}}{q}. \end{aligned} \tag{3.9}$$

Then from Lemma 2.11, Remark 2.1 and (3.9), it follows that

$$N(f_1 = 1) = \begin{cases} q^2 + 17q + 36r^2 + 18r, & \text{if } q \equiv 1 \pmod 8, \\ q^2 + 17q + 36r^2 - 30r + 4, & \text{if } q \equiv 5 \pmod 8, \end{cases} \tag{3.10}$$

$$N(f_1 = g) = \begin{cases} q^2 - 7q + 18r \pm 12r\sqrt{q - 9r^2}, & \text{if } q \equiv 1 \pmod 8, \\ q^2 - 7q + 18r - 12 \pm 4(3r - 2)\sqrt{q - (3r - 2)^2}, & \text{if } q \equiv 5 \pmod 8, \end{cases} \tag{3.11}$$

$$N(f_1 = g^2) = \begin{cases} q^2 - 3q - 36r^2 + 18r, & \text{if } q \equiv 1 \pmod 8, \\ q^2 - 3q - 36r^2 + 66r - 28, & \text{if } q \equiv 5 \pmod 8 \end{cases} \tag{3.12}$$

and

$$N(f_1 = g^3) = \begin{cases} q^2 - 7q + 18r \mp 12r\sqrt{q - 9r^2}, & \text{if } q \equiv 1 \pmod 8, \\ q^2 - 7q + 18r - 12 \mp 4(3r - 2)\sqrt{q - (3r - 2)^2}, & \text{if } q \equiv 5 \pmod 8. \end{cases} \tag{3.13}$$

as required. So part (ii) of Theorem 1.2 is proved.

This concludes the proof of Theorem 1.2. □

Now we turn our attention to the proof of Theorem 1.3.

Proof of Theorem 1.3. (i). Let $p \equiv 1 \pmod 4$. Then applying Lemma 2.10 to $n = 4$ gives us that

$$\begin{aligned} &N(f_2 = c) \\ &= q^3 + \frac{1}{q}\sum_{x \in \mathbb{F}_q^*} \left(\overline{\varphi}(x)G(\varphi, \psi_1) + \left(\frac{\mathbb{N}(x)}{p}\right)(-1)^{s-1}q^{\frac{1}{2}} + \varphi(-x)\overline{G(\varphi, \psi_1)}\right)^4 \psi_1(-xc). \end{aligned} \tag{3.14}$$

Let

$$T'_x := \left(\overline{\varphi}(x)G(\varphi, \psi_1) + \left(\frac{\mathbb{N}(x)}{p}\right)(-1)^{s-1}q^{\frac{1}{2}} + \varphi(-x)\overline{G(\varphi, \psi_1)}\right)^4 \psi_1(-xc).$$

Since

$$\varphi^2(x) = \overline{\varphi}^2(x) = \left(\frac{\mathbb{N}(x)}{p}\right), \quad \varphi^3 = \overline{\varphi}, \quad \varphi^4(x) = \overline{\varphi}^4(x) = 1,$$

it follows from Lemma 2.1 that

$$\begin{aligned}T'_x &= \psi_1(-xc)\Big(G^4(\varphi,\psi_1)+q^2+\overline{G^4(\varphi,\psi_1)}\\
&+4(-1)^{s-1}q^{\frac{1}{2}}\overline{\varphi}(x)G^3(\varphi,\psi_1)+4\varphi(-1)\varphi^2(x)qG^2(\varphi,\psi_1)\\
&+4(-1)^{s-1}q^{\frac{3}{2}}\varphi(x)G(\varphi,\psi_1)+4(-1)^{s-1}q^{\frac{3}{2}}\overline{\varphi}(x)\overline{G(\varphi,\psi_1)}\\
&+4q\varphi(-1)\varphi^2(x)\overline{G^2(\varphi,\psi_1)}+4(-1)^{s-1}q^{\frac{1}{2}}\varphi(-x)\overline{G^3(\varphi,\psi_1)}\\
&+6q\varphi^2(x)G^2(\varphi,\psi_1)+6q^2+6q\varphi^2(x)\overline{G^2(\varphi,\psi_1)}\\
&+12(-1)^{s-1}q^{\frac{3}{2}}\varphi(-x)G(\varphi,\psi_1)+12q^2\varphi(-1)+12(-1)^{s-1}q^{\frac{3}{2}}\overline{\varphi}(x)\overline{G(\varphi,\psi_1)}\Big).\end{aligned}$$

Then from the following identities

$$\varphi(x)=\frac{\varphi(-1)}{\varphi(c)}\varphi(-xc),\quad \overline{\varphi}(x)=\frac{\varphi(-1)}{\overline{\varphi}(c)}\overline{\varphi}(-xc),$$

we deduce that

$$\begin{aligned}T'_x &= \psi_1(-xc)\Big(G^4(\varphi,\psi_1)+q^2+\overline{G^4(\varphi,\psi_1)}\\
&+4(-1)^{s-1}\frac{\varphi(-1)}{\overline{\varphi}(c)}\overline{\varphi}(-xc)G^3(\varphi,\psi_1)q^{\frac{1}{2}}+\varphi(-1)\frac{4}{\varphi^2(c)}\varphi^2(-xc)G^2(\varphi,\psi_1)q\\
&+4(-1)^{s-1}\frac{\varphi(-1)}{\varphi(c)}\varphi(-xc)G(\varphi,\psi_1)q^{\frac{3}{2}}+4(-1)^{s-1}\frac{\varphi(-1)}{\overline{\varphi}(c)}\overline{\varphi}(-xc)\overline{G(\varphi,\psi_1)}q^{\frac{3}{2}}\\
&+\varphi(-1)\frac{4}{\varphi^2(c)}\varphi^2(-xc)\overline{G^2(\varphi,\psi_1)}q+(-1)^{s-1}\frac{4}{\varphi(c)}\varphi(-xc)\overline{G^3(\varphi,\psi_1)}q^{\frac{1}{2}}\\
&+\frac{6}{\varphi^2(c)}\varphi^2(-xc)G^2(\varphi,\psi_1)q+6q^2+\frac{6}{\varphi^2(c)}\varphi^2(-xc)\overline{G^2(\varphi,\psi_1)}q\\
&+(-1)^{s-1}\frac{12}{\varphi(c)}\varphi(-xc)G(\varphi,\psi_1)q^{\frac{3}{2}}+12q^2\varphi(-1)\\
&+12(-1)^{s-1}\frac{\varphi(-1)}{\overline{\varphi}(c)}\overline{\varphi}(-xc)\overline{G(\varphi,\psi_1)}q^{\frac{3}{2}}\Big).\end{aligned}\tag{3.15}$$

Since $-xc$ run through $\mathbb{F}_q^*$ whenever x run through $\mathbb{F}_q^*$ and

$$\frac{1}{\varphi(c)}=\overline{\varphi}(c),\quad \overline{\varphi}^2(c)=\varphi^2(c),$$

if follows from (3.14), (3.15), Lemmas 2.1 and Lemma 2.2 that

$$\begin{aligned}N(f_2=c) &= q^3+\frac{1}{q}\sum_{x\in\mathbb{F}_q^*}T'_x\\
&=\Big(q^3-5q-12\varphi(-1)q\Big)-\frac{1}{q}\Big(G^2(\varphi,\psi_1)+\overline{G^2(\varphi,\psi_1)}\Big)^2\\
&+\Big(4\varphi(c)+4\varphi(-1)\varphi^2(c)+4\varphi(-1)\overline{\varphi}(c)+6\varphi^2(c)+12\overline{\varphi}(c)\Big)(-1)^{s-1}q^{\frac{1}{2}}G^2(\varphi,\psi_1)\\
&+\Big(4\overline{\varphi}(c)+4\varphi(-1)\varphi^2(c)+4\varphi(-1)\varphi(c)+6\varphi^2(c)+12\varphi(c)\Big)(-1)^{s-1}q^{\frac{1}{2}}\overline{G^2(\varphi,\psi_1)}.\end{aligned}\tag{3.16}$$

But $\varphi(1) = \overline{\varphi(1)} = 1$. By (3.16) we have

$$N(f_2 = 1) = \Big(q^3 - 5q - 12\varphi(-1)q\Big) - \frac{1}{q}\Big(G^2(\varphi,\psi_1) + \overline{G^2(\varphi,\psi_1)}\Big)^2 + (-1)^{s-1}q^{\frac{1}{2}}\Big(22 + 8\varphi(-1)\Big)\Big(G^2(\varphi,\psi_1) + \overline{G^2(\varphi,\psi_1)}\Big),$$

and by (3.4), one has

$$N(f_2 = 1) = \Big(q^3 - 5q - 12\varphi(-1)q\Big) - 4a^2 + (-1)^{s-1}2aq\Big(22 + 8\varphi(-1)\Big).$$

Thus using Corollary 2.1 gives us that

$$N(f_2 = 1) = \begin{cases} q^3 - (60a + 17)q - 4a^2, & \text{if } s \text{ is even,} \\ q^3 + (60a - 17)q - 4a^2, & \text{if } p \equiv 1 \pmod 8 \text{ and } s \text{ is odd,} \\ q^3 + (4a + 1)7q - 4a^2, & \text{if } p \equiv 5 \pmod 8 \text{ and } s \text{ is odd.} \end{cases} \tag{3.17}$$

From (3.16) and $\varphi(g) = \mathrm{i}$ we know that

$$\begin{aligned} N(f_2 = g) &= \Big(q^3 - 5q - 12\varphi(-1)q\Big) - 4a^2 \\ &\quad + (-1)^{s-1}q^{\frac{1}{2}}\Big(-4\varphi(-1) - 6 - 8\mathrm{i} - 4\varphi(-1)\mathrm{i}\Big)G^2(\varphi,\psi_1) \\ &\quad + (-1)^{s-1}q^{\frac{1}{2}}\Big(-4\varphi(-1) - 6 + 8\mathrm{i} + 4\varphi(-1)\mathrm{i}\Big)\overline{G^2(\varphi,\psi_1)} \\ &= \Big(q^3 - 5q - 12\varphi(-1)q\Big) - 4a^2 \\ &\quad + (-1)^{s-1}q^{\frac{1}{2}}\Big(-4\varphi(-1) - 6\Big)\Big(G^2(\varphi,\psi_1) + \overline{G^2(\varphi,\psi_1)}\Big) \\ &\quad + (-1)^{s-1}q^{\frac{1}{2}}\Big(4\varphi(-1) + 8\Big)\mathrm{i}\Big(G^2(\varphi,\psi_1) - \overline{G^2(\varphi,\psi_1)}\Big). \end{aligned}$$

Also (3.4) gives that

$$\begin{aligned} N(f_2 = g) &= \Big(q^3 - 5q - 12\varphi(-1)q\Big) - 4a^2 \\ &\quad - (-1)^{s-1}2aq\Big(4\varphi(-1) + 6\Big) + (-1)^{s-1}2bq\Big(4\varphi(-1) + 8\Big). \end{aligned}$$

Thus using Corollary 2.1 tells us that

$$N(f_2 = g) = \begin{cases} q^3 + (20a - 24b - 17)q - 4a^2, & \text{if } s \text{ is even,} \\ q^3 - (20a - 24b + 17)q - 4a^2 & \text{if } p \equiv 1 \pmod 8 \text{ and } s \text{ is odd,} \\ q^3 - (4a - 8b - 7)q - 4a^2, & \text{if } p \equiv 5 \pmod 8 \text{ and } s \text{ is odd.} \end{cases} \tag{3.18}$$

In the similar way, noting that $\varphi(g^2) = -1$ and $\varphi(g^3) = -\mathrm{i}$, one can easily deduce that

$$N(f_2 = g^2) = \begin{cases} q^3 + (20a - 17)q - 4a^2, & \text{if } s \text{ is even,} \\ q^3 - (20a + 17)q - 4a^2, & \text{if } p \equiv 1 \pmod 8 \text{ and } s \text{ is odd,} \\ q^3 - (20a - 7)q - 4a^2, & \text{if } p \equiv 5 \pmod 8 \text{ and } s \text{ is odd.} \end{cases} \tag{3.19}$$

$$N(f_2=g^3)=\begin{cases}q^3+(20a+24b-17)q-4a^2, & \text{if } s \text{ is even},\\ q^3-(20a+24b+17)q-4a^2, & \text{if } p\equiv 1 \pmod 8 \text{ and } s \text{ is odd},\\ q^3-(4a+8b-7)q-4a^2, & \text{if } p\equiv 5 \pmod 8 \text{ and } s \text{ is odd}.\end{cases} \tag{3.20}$$

Combining (3.17) to (3.20) concludes the proof of part (i) of Theorem 1.3.

(ii). Let $p\equiv 3 \pmod 4$ and $q\equiv 1 \pmod 4$. Then s is even. From Corollary 2.1, Lemma 2.11 and (3.16), one derives that

$$N(f_2=c)=\begin{cases}q^3-17q-(4\varphi(c)+10\varphi^2(c)+16\overline{\varphi}(c))\sqrt{q}G^2(\varphi,\psi_1)\\ -(4\overline{\varphi}(c)+10\varphi^2(c)+16\varphi(c))\sqrt{q}\overline{G^2(\varphi,\psi_1)}-36r^2, & \text{if } q\equiv 1 \pmod 8,\\ q^3-17q-(4\varphi(c)+10\varphi^2(c)+16\overline{\varphi}(c))\sqrt{q}G^2(\varphi,\psi_1)\\ -(4\overline{\varphi}(c)+10\varphi^2(c)+16\varphi(c))\sqrt{q}\overline{G^2(\varphi,\psi_1)}-(6r-4)^2, & \text{if } q\equiv 5 \pmod 8.\end{cases} \tag{3.21}$$

From Lemma 2.11 and Remark 2.1, we have

$$N(f_2=1)=\begin{cases}q^3-17q-36r^2-180rq, & \text{if } q\equiv 1 \pmod 8,\\ q^3+103q-(6r-4)^2-180rq, & \text{if } q\equiv 5 \pmod 8,\end{cases} \tag{3.22}$$

$$N(f_2=g)=\begin{cases}q^3-17q-36r^2+60rq\mp 24q\sqrt{q-9r^2}, & \text{if } q\equiv 1 \pmod 8,\\ q^3-57q-(6r-4)^2+60rq\mp 24q\sqrt{q-(3r-2)^2}, & \text{if } q\equiv 5 \pmod 8,\end{cases} \tag{3.23}$$

$$N(f_2=g^2)=\begin{cases}q^3-17q-36r^2+60rq, & \text{if } q\equiv 1 \pmod 8,\\ q^3-57q-(6r-4)^2+60rq, & \text{if } q\equiv 5 \pmod 8\end{cases} \tag{3.24}$$

and

$$N(f_2=g^3)=\begin{cases}q^3-17q-36r^2+60rq\pm 24q\sqrt{q-9r^2}, & \text{if } q\equiv 1 \pmod 8,\\ q^3-57q-(6r-4)^2+60rq\pm 24q\sqrt{q-(3r-2)^2}, & \text{if } q\equiv 5 \pmod 8.\end{cases} \tag{3.25}$$

Finally, combining (3.22) to (3.25), we arrive at the results given in part (ii) of Theorem 1.3. This finishes the proof of Theorem 1.3. □

4. Two Examples

In this section, we give two examples to demonstrate the validity of our main results.

Example 4.1. *Let $N(c)$ be the number of $\mathbb{F}_5$-rational points of the affine hypersurface $x_1^4+x_2^4+x_3^4+x_4^4=c$ with $c\in\mathbb{F}_5^*$. It is easy to see that 2 is a generator of $\mathbb{F}_5^*$, $\mathrm{ind}_2(1)\equiv 0 \pmod 4$, $\mathrm{ind}_2(2)\equiv 1 \pmod 4$ and $s=1$. From Theorem 1.3, we can deduce that $a=-1$, $b=-2$, $N(1)=16$ and $N(2)=96$.*

On the other hand, by Matlab, one can calculate that

$$N(1)=\sharp\{(k,0,0,0),(0,k,0,0),(0,0,k,0),(0,0,0,k),k\in\mathbb{F}_5^*\}=16$$

and

$$N(2) = \sharp\{(k_1, k_2, 0, 0), (k_1, 0, k_2, 0), (k_1, 0, 0, k_2), (0, k_1, k_2, 0), (0, k_1, 0, k_2), (0, 0, k_1, k_2),$$
$$k_j \in \mathbb{F}_5^*, j = 1, 2\} = 96$$

which coincide with the results in Theorem 1.3.

Example 4.2. *Let $N(c)$ be the number of $\mathbb{F}_{25}$-rational points of the affine hypersurface $x_1^4+x_2^4+x_3^4+x_4^4 = c$ with $c \in \mathbb{F}_{25}^*$. Observe that $x^2 - 2$ is irreducible over $\mathbb{F}_5$. Let α be a root of $x^2 - 2$ over its split field. Then $\mathbb{F}_5(\alpha)$ is a extensive field of $\mathbb{F}_5$ with 25 elements and denoted by $\mathbb{F}_{25}$. One can write*

$$\mathbb{F}_{25} = \{x + y\alpha \mid x \in \mathbb{F}_5, y \in \mathbb{F}_5\}.$$

The additivity and multiplicity of $\mathbb{F}_{25}$ are defined as follows: $\forall\ x_i + y_i \in \mathbb{F}_{25}$ with $i = 1, 2$, define

$$(x_1 + y_1\alpha) + (x_2 + y_2\alpha) := ((x_1 + x_2) \pmod 5) + \Big((y_1 + y_2) \pmod 5\Big)\alpha$$

and

$$(x_1 + y_1\alpha)(x_2 + y_2\alpha) := (x_1x_2 + 2y_1y_2) \pmod 5 + \Big((x_1y_2 + x_2y_1) \pmod 5\Big)\alpha.$$

By Matlab, we get that $2 + 4\alpha$ is a generator of $\mathbb{F}_{25}$, $\mathrm{ind}_{2+4\alpha}(1) \equiv 0 \pmod 4$, $\mathrm{ind}_{2+4\alpha}(\alpha) \equiv 3 \pmod 4$, and $(2 + 4\alpha)^6 = 2$.

Now letting $s = 2$, $a' = -1$ and $b' = -2$ in Theorem 1.3, one obtains that $a = -3$, $b = 4$, $N(1) = 19664$ and $N(\alpha) = 16064$. This coincide with the results for $N(1)$ and $N(2)$ gotten by Matlab.

Acknowledgments

The authors thank the anonymous referees for helpful comments and suggestions. S. F. Hong was supported partially by National Science Foundation of China Grant #11771304.

Conflict of interest

We declare that we have no conflict of interest.

References

1. A. Adolphson and S. Sperber, *p-Adic estimates for exponential sums and the theorem of Chevalley-Warning*, Ann. Sci.'Ecole Norm. Sup., **20** (1987), 545–556.
2. S. Akiyama, *On the pure Jacobi sums*, Acta Arith., **75** (1996), 97–104.
3. T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
4. J. Ax, *Zeros of polynomials over finite fields*, Amer. J. Math., **86** (1964), 255–261.
5. B. Berndt, R. Evans, K. Williams, *Gauss and Jacobi Sums*, Wiley-Interscience, New York, 1998.
6. W. Cao, *A special degree reduction of polynomials over finite fields with applications*, Int. J. Number Theory, **7** (2011), 1093–1102.

7. W. Cao and Q. Sun, *On a class of equations with special degrees over finite fields*, Acta Arith., **130** (2007), 195–202.
8. S. Chowla, J. Cowles and M. Cowles, *On the number of zeros of diagonal cubic forms*, J. Number Theory, **9** (1977), 502–506.
9. L. Carlitz, *The numbers of solutions of a particular equation in a finite field*, Publ. Math. Debrecen, **4** (1956), 379–383.
10. S. N. Hu, S. F. Hong and W. Zhao, *The number of rational points of a family of hypersurfaces over finite fields*, J. Number Theory, **156** (2015), 135–153.
11. S. N. Hu and J. Y. Zhao, *The number of rational points of a family of algebraic varieties over finite fields*, Algebra Colloq., **24** (2017), 705–720.
12. H. Huang, W. Gao and W. Cao, *Remarks on the number of rational points on a class of hypersurfaces over finite fields*, Algebra Colloq., **25** (2018), 533–540.
13. K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Second Edition, Springer-Verlag, New York, 1990.
14. N. Jacobson, *Basic Algebra I*, Freeman, New York, 1985.
15. R. Lidl, H. Niederreiter, *Finite Fields*, second ed., Encyclopedia Math. Appl., Cambridge University Press, Cambridge, 1997.
16. O. Moreno and C. J. Moreno, *Improvement of Chevalley-Warningandthe Ax-Katz theorem*, Amer. J. Math., **117** (1995), 241–244.
17. G. Myerson, *On the number of zeros of diagonal cubic forms*, J. Number Theory, **11** (1979), 95–99.
18. G. Myerson, *Period polynomials and Gauss sums for finite fields*, Acta Arith., **39** (1981), 251–264.
19. W. M. Schmidt, *Equatuions over Finite Fields*, An Elementary Approach, Springer Verlag, Berlin-Heidelberg-New York, 1976.
20. T. Storer, *Cyclotomy and Difference Sets*, Chicago, IL: Marham, 1967.
21. A. Weil, *On some exponential sums*, Proc. Natu. Acad. Sci., **34** (1948), 204–207.
22. J. Wolfmann, *The number of solutions of certain diagonal equations over finite fields*, J. Number Theory, **42** (1992), 247–257.
23. W. P. Zhang and J. Y. Hu, *The number of solutions of the diagonal cubic congruence equation mod p*, Math. Rep. (Bucur.), **20** (2018), 73–80.
24. J. Y. Zhao and Y. Zhao, *On the number of solutions of two-variable diagonal quartic equations over finite fields*, AIMS Math., in press.

AIMS Press