AIMS Mathematics

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

AIMS Mathematics, 5(4): 2979–2991.
DOI:10.3934/math.2020192
Received: 16 November 2019
Accepted: 16 March 2020
Published: 20 March 2020

Research article

On the number of solutions of two-variable diagonal quartic equations over finite fields

Junyong Zhao[1,2,*] **, Yang Zhao**[3] **and Yujun Niu**[1]

[1] School of Mathematics and Statistics, Nanyang Institute of Technology, Nanyang 473004, P. R. China

[2] Mathematical College, Sichuan University, Chengdu 610064, P. R. China

[3] Nanyang Normal University, Nanyang 473061, P. R. China

* **Correspondence:** Email: jyzhao_math@163.com.

Abstract: Let p be a odd prime number and let $\mathbb{F}_q$ be the finite field of characteristic p with q elements. In this paper, by using the Gauss sum and Jacobi sum, we give an explicit formula for the number $N(x_1^4 + x_2^4 = c)$ of solutions of the following two-variable diagonal quartic equations over $\mathbb{F}_q$: $x_1^4 + x_2^4 = c$ with $c \in \mathbb{F}_q^*$. From this result, one can deduce that $N(x_1^4 + x_2^4 = c) = q + O(q^{\frac{1}{2}})$.

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

1. Introduction

Let p be an odd prime number with $q = p^s$, $s \in \mathbb{Z}^+$. Let $\mathbb{F}_q$ be the finite field of q elements. For any polynomial $f(x_1, \cdots, x_n)$ over $\mathbb{F}_q$ with n variables, we let $N(f = 0)$ stand for the number of $\mathbb{F}_q$-rational points on the affine hypersurface $f(x_1, \cdots, x_n) = 0$ over $\mathbb{F}_q^n$. That is, we have

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

Calculating the value of $N(f = 0)$ is a main topic in finite fields. Weil [15] proposed his famous conjecture on the number of rational points of the nonsingular projective hypersurface over $\mathbb{F}_q^n$. However, 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. Some works were done by Ax [3], Adolphson and Sperber [1, 2], Carlitz [5], Hong [7–9], Hu, Hong and Zhao [11] , Zhao, Hong and Zhu [17]. It is noticed that the p-adic method is used by Hong et al. in [10] to establish the universal Kummer congruences.

On the other hand, in 1977, Chowla, Cowles and Cowles [6] determined the number of solutions of the equation

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

in $\mathbb{F}_p$. In 1981, Myerson [13] extend the result in [6] to the field $\mathbb{F}_q$ and first studied the number of solution of the equation

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

over $\mathbb{F}_q$. In 2018, Zhang and Hu [16] determined an explicit formula of equation

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

with $p \equiv 1 \pmod 3$ as follows: Let $N(c)$ be the number of solutions 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 $F_p^* = \langle g \rangle$. Then they proved the following formula:

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

In this paper, we investigate the question of counting the number of solutions of the following equation:

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

with $c \in \mathbb{F}_q^*$. Actually, we obtain the following result.

Theorem 1.1. *Let $F = \mathbb{F}_q$ be the finite field with $q = p^s$ where p is an odd prime and $s \in \mathbb{Z}^+$. Let $c \in \mathbb{F}_q^*$ and g be a primitive element of $\mathbb{F}_q^*$.*

(i). *If $p \equiv 1 \pmod 8$ or $p \equiv 5 \pmod 8$ and s is even, then*

$$N(x_1^4 + x_2^4 = c) = \begin{cases} q + 6a(-1)^{s-1} - 3, & \text{if } \text{ind}_g(c) \equiv 0 \pmod 4, \\ q + 2(-1)^s(a - 2b) - 3, & \text{if } \text{ind}_g(c) \equiv 1 \pmod 4, \\ q + 2a(-1)^s - 3, & \text{if } \text{ind}_g(c) \equiv 2 \pmod 4, \\ q + 2(-1)^s(a + 2b) - 3, & \text{if } \text{ind}_g(c) \equiv 3 \pmod 4. \end{cases}$$

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

$$N(x_1^4 + x_2^4 = c) = \begin{cases} q - 2a(-1)^{s-1} + 1, & \text{if } \text{ind}_g(c) \equiv 0 \pmod 4, \\ q + 2(-1)^s(a + 2b) + 1, & \text{if } \text{ind}_g(c) \equiv 1 \pmod 4, \\ q + 6a(-1)^{s-1} + 1, & \text{if } \text{ind}_g(c) \equiv 2 \pmod 4, \\ q + 2(-1)^s(a - 2b) + 1, & \text{if } \text{ind}_g(c) \equiv 3 \pmod 4, \end{cases}$$

where $a + b\text{i} = (a' + b'\text{i})^s$ with 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). *If $p \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$, then*

$$N(x_1^4 + x_2^4 = c)$$

$$= (q-1-2\varphi(-1)+6r\eta(c)(-1)^{s-1})+2\sqrt{q-9r}(-1)^{s-1}\Big((\pm\overline{\varphi}(-c))+(\mp\varphi(-c))\Big)\mathrm{i},$$

where r is uniquely determined by

$$q = r^2+4t^2, r\equiv 1 \pmod 4, \textit{and, if } p\equiv 1 \pmod 4, \textit{ then } (r,p)=1.$$

(iii). *If* $p\equiv 3 \pmod 4$ *and* $q\equiv 3 \pmod 4$, *then*

$$N(x_1^4+x_2^4=c) = q+1.$$

We notice that Theorem 1.1 (i) for the special case $q = p$ has been mentioned in the book of Jacobsthal's book. Furthermore, Theorem 1.1 (ii) is a special case of Wolfmann [14], but we here get it by a different method. From Theorem 1.1, we can easily deduce the following statement.

Corollary 1.1. *Let* $F = \mathbb{F}_q$ *be the finite field with* $q = p^s$, *where* $p\equiv 1 \pmod 4$ *is an odd prime and* $s\in\mathbb{Z}^+$. *Let* $c\in\mathbb{F}_q^*$. *Then each of the following is true.*

(i). *If* $p\equiv 1 \pmod 4$, *then* $|N(x_1^4+x_2^4=c)-q|\le 7\sqrt{q}$ *for each* $q\ge 9$.

(ii). *If* $p\equiv 3 \pmod 4$ *and* $q\equiv 1 \pmod 4$, *then* $|N(x_1^4+x_2^4=c)-q|\le (7+4\sqrt{2})\sqrt{q}$ *for each* $q\ge 81$.

This paper is organized as follows. First of all, in Section 2, we present several basic concepts including the Gauss sums, and give some preliminary lemmas. Then in Section 3, we give the proof of our main result Theorem 1.1 and Corollary 1.2. Finally, in Section 4, we supply two examples.

2. Preliminaries

In this section, we present several definitions and auxiliary lemmas that are needed in the proof of Theorem 1.1. We begin with three definitions.

Definition 2.1. *Let p be a prime number and* $q = p^s$ *with s being a positive integer. Let* α *be an element of* $\mathbb{F}_q$. *Then the trace and norm of* α *relative to* $\mathbb{F}_p$ *are defined by*

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

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.*

Definition 2.2. *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*

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

Definition 2.3. *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 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

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

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

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

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 $x \in \mathbb{F}_q$. Let η be the quadratic character of $\mathbb{F}_q$.

We give several basic identities about Gauss sums as follows.

Lemma 2.1. *[12] 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). $|G(\chi, \psi)| = q^{1/2}$ *for* $\chi \neq \chi_0$ *and* $\psi \neq \psi_0$.

Lemma 2.2. *[12] Let $\mathbb{F}_q$ be a finite field with $q = p^s$, where p is an odd prime and $s \in \mathbb{N}_+$. Then*

$$G(\eta, \psi_1) = \begin{cases} (-1)^{s-1} q^{\frac{1}{2}}, & \text{if } p \equiv 1 \pmod 4, \\ (-1)^{s-1} \mathrm{i}^s q^{\frac{1}{2}}, & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

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. *[12] 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.

For a multiplicative character χ of $\mathbb{F}_q$, we obviously have $\chi(-1) = \pm 1$. The value $\chi(-1)$ is of interest. The following result is regarding the sign of $\chi(-1)$.

Lemma 2.4. *[12] 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.*

Clearly, we have the following consequence.

Corollary 2.1. *Let $p \equiv 1 \pmod 4$ be an odd prime and $q = p^s$ with s being a positive integer. Let φ be a multiplicative character of $\mathbb{F}_q$ of order 4. Then*

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

Proof. This corollary follows immediately from Lemma 2.4. □

Let $\widehat{\mathbb{F}_q^*}$ be the dual group consisting of all multiplicative characters of $\mathbb{F}_q^*$ with the generator φ. 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 $\gcd(t', d) = 1$. Furthermore, the number of multiplicative character λ with order d is $\phi(d)$, where ϕ is Euler's totient function. We also need the following result.

Lemma 2.5. *Let λ be a multiplicative character of $\mathbb{F}_q$ with order* $\gcd(4, q-1)$. *Then*

$$N(x^4 = b) = \sum_{j=0}^{\gcd(4,q-1)-1} \lambda^j(b).$$

Proof. We divide this into the following three cases. Let λ be any multiplicative character of $\mathbb{F}_q$ with order $d := \gcd(4, q-1)$.

Case 1. $b = 0$. Then $x^4 = 0$ has only zero solution $x = 0$ in $\mathbb{F}_q$. That is, one has $N(x^4 = 0) = 1$. Since $\lambda^0(0) = 1$ and $\lambda^j(0) = 0$ for $1 \le j \le d-1$, it follows that

$$\sum_{j=0}^{d-1} \lambda^j(0) = 1 = N(x^4 = 0)$$

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

Case 2. $b \neq 0$ and $x^4 = b$ has a solution in $\mathbb{F}_q$. Let $b = g^k$ and $x = g^y$. Then $x^4 = b$ is equivalent to the congruence

$$4y \equiv k \pmod{q-1}. \tag{2.1}$$

Then the congruence (2.1) has exactly $d = \gcd(4, q-1)$ solutions y. Hence $x^4 = b$ has exactly d solutions in $\mathbb{F}_q$. Namely, $N(x^4 = b) = d$.

Let x_0 be an element of $\mathbb{F}_q$ with $x_0^4 = b$. For any integer j with $0 \le j \le d-1$, since $d|4$ implying that $\lambda^4 = \chi_0$, the trivial multiplicative character, we have

$$\lambda^j(b) = \lambda^j(x_0^4) = (\lambda^4(x_0))^j = 1.$$

Therefore one derives that

$$\sum_{j=0}^{d-1} \lambda^j(b) = \sum_{j=0}^{d-1} 1 = d = N(x^4 = b)$$

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

Case 3. $b \neq 0$ and $x^4 = b$ has no solution in $\mathbb{F}_q$. Then $N(x^4 = b) = 0$ 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

$$\sum_{j=0}^{d-1} \lambda^j(b) = 0 = N(x^4 = b)$$

as required. Part (i) is proved in this case.

This finishes the proof of Lemma 2.5. □

The following relation between the Gauss sum $G(\chi', \psi')$ of $\mathbb{F}_p$ and the Gauss sum $G(\chi, \psi)$ of $\mathbb{F}_q$ is due to Hasse and Davenport.

Lemma 2.6. *[12] 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*

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

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

Lemma 2.7. *[4] 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 $b' \equiv a'\theta^{\frac{p-1}{4}} \pmod p$.

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 2.8. *[12] 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.*

3. Proofs of Theorems 1.1

In this section, we present the proof of Theorem 1.1 as follows.

Proof of Theorem 1.1. (i). Let $p \equiv 1 \pmod 4$. 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

$$\begin{aligned} N(x_1^4 + x_2^4 = c) &= \frac{1}{q} \sum_{x \in \mathbb{F}_q} \sum_{(x_1, x_2) \in \mathbb{F}_q^2} \exp\Big(\frac{2\pi \mathrm{i}\, \mathrm{Tr}(x(x_1^4 + x_2^4 - c))}{p}\Big) \\ &= \frac{1}{q} \sum_{x \in \mathbb{F}_q} \Big(\sum_{y \in \mathbb{F}_q} \exp\Big(\frac{2\pi \mathrm{i}\, \mathrm{Tr}(xy^4)}{p}\Big)\Big)^2 \exp\Big(\frac{2\pi \mathrm{i}\, \mathrm{Tr}(-xc)}{p}\Big) \end{aligned}$$

$$= q + \frac{1}{q}\sum_{x\in\mathbb{F}_q^*}\Big(\sum_{y\in\mathbb{F}_q}\exp\big(\frac{2\pi\mathrm{i}\,\mathrm{Tr}(xy^4)}{p}\big)\Big)^2\psi_1(-xc). \tag{3.1}$$

Denote

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

Then by Lemma 2.5, we get

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

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

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

Noticing 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

$$R_x = \overline{\varphi}(x)G(\varphi,\psi_1) + \Big(\frac{\mathbb{N}(x)}{p}\Big)(-1)^{s-1}\sqrt{q} + \varphi(-x)\overline{G(\varphi,\psi_1)}. \tag{3.2}$$

From (3.1)) and ((3.2), we derive that

$$\begin{aligned} &N(x_1^4 + x_2^4 = c) \\ &= q + \frac{1}{q}\sum_{x\in\mathbb{F}_q^*}\Big(\overline{\varphi}(x)G(\varphi,\psi_1) + \Big(\frac{\mathbb{N}(x)}{p}\Big)(-1)^{s-1}\sqrt{q} + \varphi(-x)\overline{G(\varphi,\psi_1)}\Big)^2\psi_1(-xc) \\ &:= q + \frac{1}{q}\sum_{x\in\mathbb{F}_q^*}T_x. \end{aligned} \tag{3.3}$$

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

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

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

$$T_x=\Big(\frac{\eta(-xc)}{\eta(-c)}(G^2(\varphi,\psi_1)+\overline{G^2(\varphi,\psi_1)})+(1+2\varphi(-1))q$$
$$+2(-1)^{s-1}\sqrt{q}(\frac{\varphi(-1)}{\varphi(c)}\varphi(-xc)G(\varphi,\psi_1)+\frac{1}{\overline{\varphi}(c)}\overline{\varphi}(-xc)\overline{G(\varphi,\psi_1)})\Big)\psi_1(-xc). \tag{3.4}$$

Since $-xc$ runs over $\mathbb{F}_q^*$ as x runs through $\mathbb{F}_q^*$, it follows from (3.3),(3.4) and the fact of $\sum\limits_{x\in\mathbb{F}_q^*}\psi_1(-xc)=-1$ that

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

Note that

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

From Lemmas 2.1 and 2.2, we have

$$N(x_1^4+x_2^4=c)=q+\frac{1}{q}\Big((-1)^{s-1}\sqrt{q}\eta(c)(G^2(\varphi,\psi_1)+\overline{G^2(\varphi,\psi_1)})-(1+2\varphi(-1))q$$
$$+2(-1)^{s-1}\sqrt{q}\varphi(-1)(\overline{\varphi}(c)G^2(\varphi,\psi_1)+\varphi(c)\overline{G^2(\varphi,\psi_1)})\Big). \tag{3.5}$$

Noting that $\varphi(1)=\overline{\varphi}(1)=1=\eta(1)$, it follows from (3.5) that

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

From Lemmas 2.2, 2.3 and 2.6-2.8, we can deduce that

$$G^2(\varphi,\psi_1)=(a'+b'\mathrm{i})^s q^{\frac{1}{2}},$$

where a' and b' are integers such that

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

Letting $a + b\mathrm{i} = (a' + b'\mathrm{i})^s$ gives us that

$$G^2(\varphi, \psi_1) + \overline{G^2(\varphi, \psi_1)} = 2a\sqrt{q}, \quad G^2(\varphi, \psi_1) - \overline{G^2(\varphi, \psi_1)} = 2b\mathrm{i}\sqrt{q}. \tag{3.6}$$

Thus

$$N(x_1^4 + x_2^4 = 1) = q + (1 + 2\varphi(-1))(2a(-1)^{s-1} - 1).$$

By Corollary 2.1, we get

$$N(x_1^4 + x_2^4 = 1) = \begin{cases} q + 6a(-1)^{s-1} - 3, & \text{if either } p \equiv 1 \pmod 8, \\ & \text{or } p \equiv 5 \pmod 8 \text{ and } s \text{ is even}, \\ q - 2a(-1)^{s-1} + 1, & \text{if } p \equiv 5 \pmod 8 \text{ and } s \text{ is odd}. \end{cases} \tag{3.7}$$

From (3.5), (3.6), $\varphi(g) = \mathrm{i}$ and $\eta(g) = -1$ we obtain that

$$N(x_1^4 + x_2^4 = g) = q + 2(-1)^s(a - 2b\varphi(-1)) - (1 + 2\varphi(-1)).$$

By Corollary 2.1, we have

$$N(x_1^4 + x_2^4 = g) = \begin{cases} q + 2(-1)^s(a - 2b) - 3, & \text{if either } p \equiv 1 \pmod 8, \\ & \text{or } p \equiv 5 \pmod 8 \text{ and } s \text{ is even}, \\ q + 2(-1)^s(a + 2b) + 1, & \text{if } p \equiv 5 \pmod 8 \text{ and } s \text{ is odd}. \end{cases} \tag{3.8}$$

From (3.5), (3.6), $\varphi(g^2) = -1$ and $\eta(g^2) = 1$, we have

$$N(x_1^4 + x_2^4 = g^2) = q + 2a(-1)^{s-1}(1 - 2\varphi(-1)) - (1 + 2\varphi(-1)).$$

By Corollary 2.1 it follows that

$$N(x_1^4 + x_2^4 = g^2) = \begin{cases} q + 2a(-1)^s - 3, & \text{if either } p \equiv 1 \pmod 8, \\ & \text{or } p \equiv 5 \pmod 8 \text{ and } s \text{ is even}, \\ q + 6a(-1)^{s-1} + 1, & \text{if } p \equiv 5 \pmod 8 \text{ and } s \text{ is odd}. \end{cases} \tag{3.9}$$

From (3.5), (3.6), $\varphi(g^3) = -\mathrm{i}$ and $\eta(g^3) = -1$, we deduce

$$N(x_1^4 + x_2^4 = g^3) = q + 2(-1)^s(a + 2b\varphi(-1)) - (1 + 2\varphi(-1)).$$

By Corollary 2.1 we have

$$N(x_1^4 + x_2^4 = g^3) = \begin{cases} q + 2(-1)^s(a + 2b) - 3, & \text{if either } p \equiv 1 \pmod 8, \\ & \text{or } p \equiv 5 \pmod 8 \text{ and } s \text{ is even}, \\ q + 2(-1)^s(a - 2b) + 1, & \text{if } p \equiv 5 \pmod 8 \text{ and } s \text{ is odd}. \end{cases} \tag{3.10}$$

From (3.7), (3.8), (3.9) and (3.10), we can conclude the proof of part (i).

(ii). Let $p \equiv 3 \pmod 4$ and $q \equiv 1 \pmod 4$. Since $p \equiv 3 \pmod 4$ implying that

$$q = p^s \equiv \begin{cases} 1 \pmod 4, & \text{if } s \text{ is even}, \\ 3 \pmod 4, & \text{if } s \text{ is odd}, \end{cases} \tag{3.11}$$

one must have that s is even. Let N_k be the number of solutions of $x_1^4 + x_2^4 + \cdots + x_k^4 = 0$ over $\mathbb{F}_q$. Myerson [13] gave the value of

$$N_2 = 4q - 3, \quad N_3 = q^2 - 6rq + 6r,$$

where r is uniquely determined by

$$q = r^2 + 4t^2, r \equiv 1 \pmod 4, \text{ and if } p \equiv 1 \pmod 4, \text{ then } (r, p) = 1.$$

Since

$$\begin{aligned} N_3 &= \sum_{\substack{(x_1,x_2,x_3)\in\mathbb{F}_q^3 \\ x_1^4+x_2^4+x_3^4=0}} 1 = \sum_{\substack{(x_1,x_2)\in\mathbb{F}_q^2 \\ x_1^4+x_2^4=0}} 1 + \sum_{\substack{x_3\in\mathbb{F}_q^* \\ x_1^4+x_2^4=-x_3^4}} 1 \\ &= N_2 + (q-1)N(x_1^4 + x_2^4 = -1), \end{aligned}$$

one has

$$N(x_1^4 + x_2^4 = -1) = \frac{N_3 - N_2}{q-1} = \frac{q^2 - (6r+4)q + 6r + 3}{q-1}. \tag{3.12}$$

From (3.11) and Corollary 2.1, we have $\varphi(-1) = 1$ if s is even.

By (3.5), one has

$$\begin{aligned} &N(x_1^4 + x_2^4 = -1) \\ &= q + \frac{1}{q}\Big((-1)^{s-1}\sqrt{q}(G^2(\varphi,\psi_1) + \overline{G^2(\varphi,\psi_1)}) - (1 + 2\varphi(-1))q\Big) \\ &= q - \frac{1}{q}\Big(\sqrt{q}(G^2(\varphi,\psi_1) + \overline{G^2(\varphi,\psi_1)}) + 3q\Big) \end{aligned} \tag{3.13}$$

From (3.12) and (3.13), we can deduce

$$G^2(\varphi,\psi_1) + \overline{G^2(\varphi,\psi_1)} = 6r\sqrt{q}.$$

Let $G^2(\varphi,\psi_1) = 3r\sqrt{q} + B\mathrm{i}$. By $G^2(\varphi,\psi_1)\overline{G^2(\varphi,\psi_1)} = q^2$, one has

$$B = \pm\sqrt{q^2 - 9r^2q}.$$

So we can write $G^2(\varphi,\psi_1) = 3r\sqrt{q} \pm \sqrt{q^2 - 9r^2q}\,\mathrm{i}$. From (3.5), one has

$$\begin{aligned} &N(x_1^4 + x_2^4 = c) \\ &= (q - 1 - 2\varphi(-1) + 6r\eta(c)(-1)^{s-1}) + 2\sqrt{q - 9r}(-1)^{s-1}\Big((\pm\overline{\varphi}(-c)) + (\mp\varphi(-c))\Big)\mathrm{i}. \end{aligned}$$

This finishes the proof of (ii).

(iii). Let $p \equiv 3 \pmod 4$ and $q \equiv 3 \pmod 4$. Since $\gcd(4, q-1) = \gcd(2, q-1)$. By Lemma 2.5, one has $N(x^4 = A) = N(x^2 = A)$. It follows that

$$N(x_1^4 + x_2^4 = c)$$

$$
\begin{aligned}
&= \sum_{\substack{(x_1,x_2)\in\mathbb{F}_q^2\\ c_1+c_2=c}} N(x_1^4=c_1)N(x_2^4=c_2)\\
&= \sum_{\substack{(x_1,x_2)\in\mathbb{F}_q^2\\ c_1+c_2=c}} N(x_1^2=c_1)N(x_2^2=c_2)\\
&= \sum_{\substack{(x_1,x_2)\in\mathbb{F}_q^2\\ c_1+c_2=c}} (1+\eta(c_1))(1+\eta(c_2))\\
&= q+\sum_{c_1\in\mathbb{F}_q}\eta(c_1)+\sum_{c_1\in\mathbb{F}_q}\eta(c_2)+\sum_{c_1\in\mathbb{F}_q}\eta(c_1c_2)\\
&= q+\sum_{x\in\mathbb{F}_q}\eta(cx-x^2)=q+\sum_{x\in\mathbb{F}_q^*}\eta(cx^{-1}-1).\\
&= q+\sum_{y\in\mathbb{F}_q^*}\eta(y-1)=q+1.
\end{aligned}
$$

This finishes the proof of part (iii), and hence that of Theorem 1.1. □

Proof of Corollary 1.2. (i). Let $q \equiv 1 \pmod 4$. From Theorem 1.1, one has $|a| \le \sqrt{q}$ and $|b| \le \sqrt{q}$, therefore one deduces that $|a \pm 2b| \le 3\sqrt{q}$. Then we derive the desired result $|N(x_1^4+x_2^4=c)-q| \le 7\sqrt{q}$ by triangle inequality.

(ii). Let $p \equiv 1 \pmod 4$ and $q \equiv 3 \pmod 4$. From Theorem 1.1, one has $|r| \le \sqrt{q}$, $\sqrt{q-9\sqrt{q}} \le \sqrt{q-9r} \le \sqrt{q+9\sqrt{q}}$ and $|\Big((\pm \overline{\varphi}(-c)) + (\mp \varphi(-c))\Big)\mathrm{i}| \le 2$. From this, we deduce that

$$
\begin{aligned}
|N(x_1^4+x_2^4=c)-q| &\le |3+6r+4\sqrt{q-4r}|\\
&\le 3+6r+4\sqrt{q+9r}\\
&\le 3+6r+4\sqrt{2q}\\
&\le (7+4\sqrt{2})\sqrt{q}
\end{aligned}
$$

as required. The proof of Corollary 1.2 is complete. □

4. Two Examples

In this final section, we provide two examples to demonstrate the validity of our main result Theorem 1.1.

Example 4.1. *For finite field $\mathbb{F}_5$, it is easy to see that 2 is a generator of $\mathbb{F}_5^*$. Note that $s = 1$. Then $a' = a = -1$ and $b' = b = -2$.*

Since $\mathrm{ind}_2(1) \equiv 0 \pmod 4$, $\mathrm{ind}_2(2) \equiv 1 \pmod 4$, $\mathrm{ind}_2(3) \equiv 3 \pmod 4$, $\mathrm{ind}_2(2) \equiv 2 \pmod 4$. *From Theorem 1.1, one can compute and get that*

$$N(x_1^4+x_2^4=1)=8, \quad N(x_1^4+x_2^4=2)=16,$$

$$N(x_1^4+x_2^4=3)=N(x_1^4+x_2^4=4)=0.$$

Example 4.2. *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 an extension field of* $\mathbb{F}_5$ *with order* 25, *and we denote it by* $\mathbb{F}_{25}$, *where*

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

For any $x_i + y_i \in \mathbb{F}_{25}$ *with* $i = 1, 2$, *we 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 programme, we confirm that the element $2 + 4\alpha$ *is a generator of* $\mathbb{F}_{25}$.

Note that $s = 2$, $a' = -1$, $b' = -2$. *Then* $a = -3$ *and* $b = 4$. *Since* $\mathrm{ind}_{2+4\alpha}(1) \equiv 0 \pmod 4$ *and* $\mathrm{ind}_{2+4\alpha}(\alpha) \equiv 3 \pmod 4$, *it follows from Theorem 1.1 that*

$$N(x_1^4 + x_2^4 = 1) = 40, \quad N(x_1^4 + x_2^4 = \alpha) = 32.$$

Acknowledgments

The authors are thankful for the anonymous referees for their careful reading of the manuscript and helpful comments. They also thank Dr. Chaoxi Zhu and Dr. Lingfeng Ao for many helpful suggestions.

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. A. Adolphson and S. Sperber, *p-Adic estimates for exponential sums*. In: F.Baldassarri, S. Bosch, B. Dwork (eds) p-adic Analysis. Lecture Notes in Mathematics, Springer, Berlin, 1990.
3. J. Ax, *Zeros of polynomials over finite fields*, Amer. J. Math., **86** (1964), 255–261.
4. B. Berndt, R. Evans, K. Williams, *Gauss and Jacobi Sums*, Wiley-Interscience, New York, 1998.
5. L. Carlitz, *The numbers of solutions of a particular equation in a finite field*, Publ. Math. Debrecen, **4** (1956), 379–383.
6. S. Chowla, J. Cowles and M. Cowles, *On the number of zeros of diagonal cubic forms*, J. Number Theory, **9** (1977), 502–506.
7. S. F. Hong, *Newton polygons of L-functions associtated with exponential sums of polynomials of degree four over finite fields*, Finite Fields Th. App., **7** (2001), 205–237.
8. S. F. Hong, *Newton polygons of L-functions associtated with exponential sums of polynomials of degree six over finite fields*, J. Number Theory, **97** (2002), 368–396.

9. S. F. Hong, *L-functions of twisted diagonal exponential sums over finite fields*, Proc. Amer. Soc., **135** (2007), 3099–3108.
10. S. F. Hong, J. R. Zhao and W. Zhao, *The universal Kummer congruences*, J. Aust. Math. Soc., **94** (2013), 106–132.
11. 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.
12. R. Lidl, H. Niederreiter, *Finite Fields*, second ed., Cambridge University Press, Cambridge, 1997.
13. G. Myerson, *On the number of zeros of diagonal cubic forms*, J. Number Theory, **11** (1979), 95–99.
14. J. Wolfmann, *The number of solutions of certain diagonal equations over finite fields*, J. Number Theory, **42** (1992), 247–257.
15. A. Weil, *On some exponential sums*, Proc. Natu. Acad. Sci., **34** (1948), 204–207.
16. 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.
17. J. Y. Zhao, S. F. Hong and C. X. Zhu, *The number of rational points of certain quartic diagonal hypersurfaces over finite fields*, AIMS Math., **5** (2020), 2710–2731.

AIMS Press