THE NUMBER OF SOLUTIONS OF THE DIAGONAL CUBIC CONGRUENCE EQUATION mod p

ZHANG WENPENG and HU JIAYUAN

Communicated by Alexandru Zaharescu

The main purpose of this paper is using the analytic methods and the properties of Gauss sums to study the computational problem of the number of the solutions of one kind diagonal cubic congruence equation mod p, an odd prime, and give an interesting calculating formula for it.

AMS 2010 Subject Classification: 11L05.

Key words: the diagonal cubic congruence equation, Gauss sums, calculating formula.

1. INTRODUCTION

Let $q \geq 3$ be a positive integer. For any integers m and n, the two-term exponential sum $C(m, n, k; q)$ is defined as follows:

$$C(m, n, k; q) = \sum_{a=1}^{q} e\left(\frac{ma^k + na}{q}\right),$$

where $e(y) = e^{2\pi iy}$, k is an integer with $k \geq 2$.

About this two-term exponential sum, some authors have studied its various properties, and obtained a series of interesting results, see [3–8]. For example, Gauss's classical work (referred in [1]) gave an exact computational formula for $C(1, 0, 2; q)$. From the A. Weil's important work [3], one can get the upper bound estimate

$$|C(m, n, k; p)| \ll_k \sqrt{p},$$

where p be an odd prime, m and n are integers with $(m, p) = 1$, and $\ll_k$ denotes the big-O constant depend only on k.

Recently, H. Zhang and W. Zhang [8] studied the calculating problem of the fourth power mean of the two-term exponential sum, and proved the following beautiful formula

$$\sum_{m=1}^{p-1}\left|\sum_{a=0}^{p-1} e\left(\frac{ma^3+na}{p}\right)\right|^4 = \begin{cases} 2p^3-p^2, & \text{if } 3\nmid p-1, \\ 2p^3-7p^2, & \text{if } 3\mid p-1, \end{cases}$$

where p is an odd prime and $(n,p)=1$.

At the same time, H. Zhang and W. Zhang [8] also proposed the following open problem:

Can the number of solutions to the cubic equation

$$x_1^3+x_2^3+x_3^3+x_4^3 \equiv c \bmod p \tag{1}$$

be calculated when $c \neq 0$?

In this paper, as a note of [8], we will give a formula for the number of solutions of equation (1). That is, we shall prove the following:

THEOREM 1. *Let p be an odd prime with $3|(p-1)$, ψ be any three order character* mod p. *Then we have the identity*

$$\tau^3(\psi)+\tau^3\left(\overline{\psi}\right)=dp,$$

where $\tau(\psi)$ denotes the classical Gauss sums, d is uniquely determined by $4p=d^2+27b^2$ and $d\equiv 1 \bmod 3$.

THEOREM 2. *Let $p>3$ be a prime with $3|(p-1)$, $S(c)$ denotes the number of solutions of the congruence equation* (1). *Then for any integer c with $(c,p)=1$, we have the identity*

$$S(c)=\begin{cases} p^3-6p-\frac{1}{2}p\left(5d\mp 27b\right), & \text{if } c\equiv g^{3k+1} \bmod p; \\ p^3-6p-\frac{1}{2}p\left(5d\pm 27b\right), & \text{if } c\equiv g^{3k+2} \bmod p; \\ p^3-6p+5dp, & \text{if } c\equiv g^{3k} \bmod p, \end{cases}$$

where g is a primitive root mod p, *d and b are defined as in Theorem 1, and k be any integer with $0\le k\le \frac{p-1}{3}$.*

Some notes. It seems that our main result (Theorem 2) cannot be generalized to any other composite number q, because in the process of the proof of Theorem 2, we used S. Chowla, J. Cowles and M. Cowles' important work [2], which is only applicable to the finite field $GF(p)$.

For any integers $k>2$ and $h>3$, there exists an exact calculating formula for the mean value

$$\sum_{m=1}^{p-1}\left|\sum_{a=1}^{p-1} e\left(\frac{ma^3+na}{p}\right)\right|^{2k} \quad \text{or} \quad \sum_{m=1}^{p-1}\left|\sum_{a=1}^{p-1} e\left(\frac{ma^h+na}{p}\right)\right|^4 ?$$

These are two interesting open problems.

Let $\psi(n) = e\left(\frac{\mathrm{ind}(n)}{3}\right)$ denotes the three order character mod p, where $\mathrm{ind}(n)$ denotes the index of n corresponding to primitive root g mod p. That is, $n \equiv g^{\mathrm{ind}(n)} \bmod p$. We also let $\tau^3(\psi) = u + iv$. In this time, we have

(A): If $v > 0$, then we have the computational formula:

$$S(c) = \begin{cases} p^3 - 6p - \frac{1}{2}p(5d - 27b), & \text{if } c \equiv g^{3k+1} \bmod p; \\ p^3 - 6p - \frac{1}{2}p(5d + 27b), & \text{if } c \equiv g^{3k+2} \bmod p. \end{cases}$$

(B): If $v < 0$, then we have the computational formula:

$$S(c) = \begin{cases} p^3 - 6p - \frac{1}{2}p(5d + 27b), & \text{if } c \equiv g^{3k+1} \bmod p; \\ p^3 - 6p - \frac{1}{2}p(5d - 27b), & \text{if } c \equiv g^{3k+2} \bmod p. \end{cases}$$

How to determine the plus or minus of v is also an interesting problem. We hope that the interested readers can study it with us.

Combining some earlier results and our Theorem 1 we may immediately deduce the following:

COROLLARY 1. *Let p be an odd prime, then we have the identity*

$$\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1} e\left(\frac{ma^3 + na}{p}\right)\right|^4 = \begin{cases} 2p^3 - 3p^2 - 3p, & \text{if } 3 \nmid p-1; \\ 2p^3 - 5p^2 - 15p + 4dp, & \text{if } 3 | p-1, \end{cases}$$

where $(n, p) = 1$, d is defined as in Theorem 1.

COROLLARY 2. *For any odd prime p with $3|(p-1)$, let $A(p)$ denotes the number of all integers $2 \le a \le p-1$ such that $a(a-1)$ is a cubic residue* mod p. *Then we have the computational formula*

$$A(p) = \frac{1}{3}(p - 2 + d).$$

2. SEVERAL LEMMAS

In this section, we will give several lemmas which are necessary in the proofs of our theorems. Hereinafter, we need some properties of Gauss sums, all of which can be found in [1], so they will not be repeated here. First we have the following:

LEMMA 1. *Let p be an odd prime with $p \equiv 1 \bmod 3$, for any integer $1 \le c \le p-1$, let $S(c)$ denotes the number of solutions of the congruence equation (1). Then we have the identity*

$$S(c) = p^3 - 6p + \psi(c)\tau^3(\psi) + 4\overline{\psi}(c)\tau^3(\psi) + 4\psi(c)\tau^3\left(\overline{\psi}\right) + \overline{\psi}(c)\tau^3\left(\overline{\psi}\right).$$

where ψ be any three order character mod p.

Proof. From the trigonometric identity

$$\sum_{m=0}^{p-1} e\left(\frac{nm}{p}\right) = \begin{cases} p, & \text{if } (p,n) = p; \\ 0, & \text{if } (p,n) = 1 \end{cases}$$

we have

$$S(c) = \frac{1}{p}\sum_{m=0}^{p-1}\left(\sum_{a=0}^{p-1} e\left(\frac{ma^3}{p}\right)\right)^4 e\left(\frac{-mc}{p}\right) = p^3 + \frac{1}{p}\sum_{m=1}^{p-1}\left(\sum_{a=0}^{p-1} e\left(\frac{ma^3}{p}\right)\right)^4 e\left(\frac{-mc}{p}\right). \tag{2}$$

For any three order character $\psi \bmod p$ and integers $1 \le m \le p-1$, note that $\psi^2 = \overline{\psi}$, from the definition and properties of Gauss sums we know that

$$\begin{aligned}\sum_{a=0}^{p-1} e\left(\frac{ma^3}{p}\right) &= 1 + \sum_{a=1}^{p-1}\left(1 + \psi(a) + \psi^2(a)\right) e\left(\frac{ma}{p}\right) \\ &= \sum_{a=0}^{p-1} e\left(\frac{ma}{p}\right) + \sum_{a=1}^{p-1}\psi(a) e\left(\frac{ma}{p}\right) + \sum_{a=1}^{p-1}\overline{\psi}(a) e\left(\frac{ma}{p}\right) \\ &= \overline{\psi}(m)\tau(\psi) + \psi(m)\tau\left(\overline{\psi}\right).\end{aligned} \tag{3}$$

Note that $\psi(-1) = 1$, $\tau(\psi)\tau\left(\overline{\psi}\right) = p$ and $\psi^3(m) = 1$, so from (3) and the definition of Gauss sums we have

$$\begin{aligned}\sum_{m=1}^{p-1}\left(\sum_{a=0}^{p-1} e\left(\frac{ma^3}{p}\right)\right)^4 e\left(\frac{-mc}{p}\right) &= \sum_{m=1}^{p-1}\left(\overline{\psi}(m)\tau(\psi) + \psi(m)\tau\left(\overline{\psi}\right)\right)^4 e\left(\frac{-mc}{p}\right) \\ &= p\psi(c)\tau^3(\psi) + 4p\overline{\psi}(c)\tau^3(\psi) - 6p^2 + 4p\psi(c)\tau^3\left(\overline{\psi}\right) + p\overline{\psi}(c)\tau^3\left(\overline{\psi}\right).\end{aligned} \tag{4}$$

Now combining (2) and (4) we have

$$S(c) = p^3 + \psi(c)\tau^3(\psi) + 4\overline{\psi}(c)\tau^3(\psi) - 6p + 4\psi(c)\tau^3\left(\overline{\psi}\right) + \overline{\psi}(c)\tau^3\left(\overline{\psi}\right).$$

This proves Lemma 1. □

Lemma 2. *Let p be an odd prime with $3|(p-1)$, M_s denotes the number of solutions of the equation*

$$X_1^3 + X_2^3 + X_3^3 + \cdots + X_s^3 = 0$$

in the finite field $GF(p)$, $U_s = M_s - p^{s-1}$. Then U_s satisfy the linear recurrence $U_s - 3pU_{s-2} - pdU_{s-3} = 0$ with $U_1 = 0$, $U_2 = 2p-2$ and $U_3 = (p-1)d$, where d is uniquely determined by $4p = d^2 + 27b^2$ and $d \equiv 1 \bmod 3$.

Proof. See Theorem 3 of [2]. □

LEMMA 3. *Let p be an odd prime with $3|(p-1)$, then we have*

$$S(1) = p^3 - 6p + 5dp.$$

Proof. From Lemma 2 we have $U_4 = 3p(2p-2) = 6p(p-1)$, $U_5 = 3pU_3 + pdU_2 = 3pd(p-1) + pd(2p-2) = 5dp(p-1)$. So from the properties of the complete residue system mod p we have

$$\begin{aligned}(5)\quad 5dp(p-1) + p^4 = U_5 + p^4 = M_5 &= \sum_{\substack{a=0\\ a^3+b^3+c^3+d^3+e^3\equiv 0 \bmod p}}^{p-1}\sum_{b=0}^{p-1}\sum_{c=0}^{p-1}\sum_{d=0}^{p-1}\sum_{e=0}^{p-1} 1\\ &= \sum_{\substack{a=0\\ a^3+b^3+c^3+d^3\equiv 0 \bmod p}}^{p-1}\sum_{b=0}^{p-1}\sum_{c=0}^{p-1}\sum_{d=0}^{p-1} 1 + \sum_{\substack{a=0\\ a^3+b^3+c^3+d^3\equiv (p-e)^3 \bmod p}}^{p-1}\sum_{b=0}^{p-1}\sum_{c=0}^{p-1}\sum_{d=0}^{p-1}\sum_{e=1}^{p-1} 1\\ &= M_4 + \sum_{e=1}^{p-1}\sum_{\substack{a=0\\ a^3+b^3+c^3+d^3\equiv 1 \bmod p}}^{p-1}\sum_{b=0}^{p-1}\sum_{c=0}^{p-1}\sum_{d=0}^{p-1} 1 = M_4 + (p-1)S(1).\end{aligned}$$

Note that $M_4 = p^3 + 6p(p-1)$, from (5) we may immediately deduce that

$$S(1) = p^3 + 5dp - 6p.$$

This proves Lemma 3. □

3. PROOF OF THE THEOREMS AND COROLLARIES

In this section, we shall complete the proofs of our theorems and corollaries. First we prove Theorem 1. Taking $c = 1$ in Lemma 1 and note that $\psi(1) = 1$, from Lemma 3 we have

$$\begin{aligned} & p^3 + 5dp - 6p = S(1)\\ = \;& p^3 - 6p + \psi(1)\tau^3(\psi) + 4\overline{\psi}(1)\tau^3(\psi) + 4\psi(1)\tau^3\left(\overline{\psi}\right) + \overline{\psi}(1)\tau^3\left(\overline{\psi}\right)\\ = \;& p^3 - 6p + 5\tau^3(\psi) + 5\tau^3\left(\overline{\psi}\right),\end{aligned}$$

or

$$\tau^3(\psi) + \tau^3\left(\overline{\psi}\right) = dp.$$

This proves Theorem 1.

Now we prove Theorem 2. Let g be any fixed primitive root mod p, $\psi(g) = e\left(\frac{1}{3}\right) = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, then $\overline{\psi}(g) = -\frac{1}{2} - \frac{\sqrt{3}}{2}i$. So from Lemma 1 and Theorem 1 we have

$$(6)\quad S(g)=p^3-6p+\psi(g)\tau^3(\psi)+4\overline{\psi}(g)\tau^3(\psi)+4\psi(g)\tau^3\left(\overline{\psi}\right)+\overline{\psi}(g)\tau^3\left(\overline{\psi}\right)$$
$$=p^3-6p+\left(-\frac{5}{2}-\frac{3\sqrt{3}}{2}i\right)\tau^3(\psi)+\left(-\frac{5}{2}+\frac{3\sqrt{3}}{2}i\right)\tau^3\left(\overline{\psi}\right)$$
$$=p^3-6p-\frac{5}{2}\left(\tau^3(\psi)+\tau^3\left(\overline{\psi}\right)\right)-\frac{3\sqrt{3}}{2}i\left(\tau^3(\psi)-\tau^3\left(\overline{\psi}\right)\right).$$

Let $\tau^3(\psi)=u+iv$, then $\tau^3\left(\overline{\psi}\right)=u-iv$. So from Theorem 1 we have $dp=\tau^3(\psi)+\tau^3\left(\overline{\psi}\right)=2u$ and $u=\frac{dp}{2}$. Note that $u^2+v^2=\left|\tau^3(\psi)\right|^2=p^3$, we have

$$(7)\qquad |v|=\frac{1}{2}p\sqrt{4p-d^2}=\frac{3\sqrt{3}}{2}bp,$$

where $4p=d^2+27b^2$.

Combining (6) and (7) we have the identity

$$(8)\qquad S(g)=p^3-6p-\frac{5}{2}dp+3\sqrt{3}v=p^3-6p-\frac{1}{2}p\left(5d\mp 27b\right).$$

Similarly, we also have

$$(9)\qquad S(g^2)=p^3-6p-\frac{5}{2}dp+3\sqrt{3}v=p^3-6p-\frac{1}{2}p\left(5d\pm 27b\right).$$

Combining (7), (8), (9) and Lemma 2 we may immediately deduce the computational formula

$$S(c)=\begin{cases} p^3-6p-\frac{1}{2}p\left(5d\mp 27b\right), & \text{if } c\equiv g^{3k+1} \bmod p;\\ p^3-6p-\frac{1}{2}p\left(5d\pm 27b\right), & \text{if } c\equiv g^{3k+2} \bmod p;\\ p^3-6p+5dp, & \text{if } c\equiv g^{3k} \bmod p,\end{cases}$$

where k be an integer with $0\le k\le\frac{p-1}{3}$.

This proves Theorem 2.

Now we prove Corollary 2. For any three order character $\psi \bmod p$, note that $\overline{\psi}^2=\psi$, $\psi(-1)=1$, $\tau(\psi)\tau\left(\overline{\psi}\right)=p$, from the properties of Gauss sums we have

$$(10)\quad \sum_{a=1}^{p-1}\psi\left(a(a-1)\right)=\frac{1}{\tau\left(\overline{\psi}\right)}\sum_{a=1}^{p-1}\psi(a)\sum_{b=1}^{p-1}\overline{\psi}(b)e\left(\frac{b(a-1)}{p}\right)$$
$$=\frac{1}{\tau\left(\overline{\psi}\right)}\sum_{b=1}^{p-1}\overline{\psi}(b)e\left(\frac{-b}{p}\right)\sum_{a=1}^{p-1}\psi(a)e\left(\frac{ba}{p}\right)=\frac{\tau(\psi)}{\tau\left(\overline{\psi}\right)}\sum_{b=1}^{p-1}\overline{\psi}^2(b)e\left(\frac{-b}{p}\right)$$
$$=\frac{\tau(\psi)}{\tau\left(\overline{\psi}\right)}\sum_{b=1}^{p-1}\psi(b)e\left(\frac{-b}{p}\right)=\frac{\tau^2(\psi)}{\tau\left(\overline{\psi}\right)}=\frac{\tau^3(\psi)}{p}.$$

Similarly, we also have

$$\sum_{a=1}^{p-1}\overline{\psi}\left(a(a-1)\right)=\frac{\tau^3\left(\overline{\psi}\right)}{p}. \tag{11}$$

Let $A(p)$ denotes the number of all integers $2\le a\le p-1$ such that $a(a-1)$ is a cubic residue mod p and $B(p)=p-2-A(p)$. Then from (10) and (11) we have

$$\sum_{a=1}^{p-1}\left[\psi\left(a(a-1)\right)+\overline{\psi}\left(a(a-1)\right)\right]=\frac{1}{p}\left[\tau^3(\psi)+\tau^3\left(\overline{\psi}\right)\right]. \tag{12}$$

For any integer n with $(n,p)=1$, note that $1+\psi(n)+\overline{\psi}(n)=3$, if n is a cubic residue mod p; and $1+\psi(n)+\overline{\psi}(n)=0$, if n is not a cubic residue mod p. So from (12), Theorem 1 and the definition of $A(p)$ and $B(p)$ we have

$$2A(p)-B(p)=\frac{1}{p}\left[\tau^3(\psi)+\tau^3\left(\overline{\psi}\right)\right]=d \tag{13}$$

Since $A(p)+B(p)=p-2$, so from (13) we may immediately deduce that

$$A(p)=\tfrac{1}{3}\left(p-2+d\right)\ \text{ and }\ B(p)=\tfrac{1}{3}\left(2p-4-d\right).$$

This completes the proof of Corollary 2.

Acknowledgments. This work is supported by the N.S.F. (11371291) of P.R. China. The authors would like to thank the referee for his very helpful and detailed comments, which have significantly improved the presentation of this paper.

REFERENCES

[1] Tom M. Apostol, *Introduction to Analytic Number Theory.* Springer-Verlag, New York, 1976.

[2] S. Chowla, J. Cowles and M. Cowles, *On the number of zeros of diagonal cubic forms.* J. Number Theory **9** (1977), 502–506.

[3] A. Weil, *On some exponential sums.* Proc. Natl. Acad. Sci. USA **34** (1948), 204–207.

[4] T. Cochrane and Z. Zheng, *Pure and mixed exponential sums.* Acta Arith. **91** (1999), 249–278.

[5] T. Cochrane and C. Pinner, *A further refinement of Mordell's bound on exponential sums.* Acta Arith. **116** (2005), 35–41.

[6] T. Cochrane and C. Pinner, *Using Stepanov's method for exponential sums involving rational functions.* J. Number Theory **116** (2006), 270–292.

[7] W. Duke and H. Iwaniec, *A relation between cubic exponential and Kloosterman sums.* Contemp. Math. **143** (1993), 255–258.

[8] Zhang Han and Zhang Wenpeng, *The fourth power mean of two-term exponential sums and its application.* Math. Rep. (Bucur.) **19(69)** (2017), *1*, 75–83.

Received 1 March 2016

Northwest University,
School of Mathematics
Xi'an, Shaanxi, P.R. China
wpzhang@nwu.edu.cn