Vol. 37 (2017)
No. 5

数 学 杂 志
J. of Math. (PRC)

AN EXPLICIT FORMULA FOR THE FOURTH MOMENT OF TWO-TERM EXPONENTIAL SUMS

AI Xiao-chuan[1], CHEN Hua[2], ZHANG Si-lan[3]

(*1.Department of Applied Mathematics, School of Science, Naval University of Engineering, Wuhan 430033, China*)

(*2.School of Science, Hubei University of Technology, Wuhan 430068, China*)

(*3.College of Science, Huazhong Agricultural University, Wuhan 430070, China*)

Abstract: The fourth power mean of two-term exponential sums is studied in this paper. By elementary and algebraic methods, an explicit computation formula and a transform formula are proposed, which extend the original research results and discover the essential relation between fourth moment and congruence equations.

Keywords: two-term exponential sums; mixed exponential mean; fourth power mean; transform formula

2010 MR Subject Classification: 11T23; 11T24

Document code: A **Article ID:** 0255-7797(2017)05-0945-11

1 Introduction

For integers m, n, q, k with $q \geq 3, k \geq 2$, we define a two-term exponential sums

$$C(m,n,k;q) = \sum_{a=1}^{q}{}' e(\frac{ma^k + na}{q}), \tag{1.1}$$

where $e(y) = e^{2\pi iy}$ and $\sum_{a=1}^{q}{}'$ denotes the summation over all a with $(a,q) = 1$. The two-term exponential sums $C(m,n,k;q)$ originally arose in connection with Waring's problem and the aim is to find optimal bounds. As a pioneer work, Davenport and Heilbronn [2] proved that

$$C(m,n,k;p^\alpha) \ll {}_k p^{\alpha\theta}(m,p^\alpha) \tag{1.2}$$

for $(p,m) = 1$, where $\theta = 2/3$ for $k = 3$ and $\theta = 3/4$ for $k > 3$. Afterwards, Hua [9] showed that $\theta = 1/2$ for all $k \geq 2$ by using Weil's estimate for exponential sums over finite fields.

* **Received date:** 2015-09-06 **Accepted date:** 2015-11-25

Foundation item: Supported by National Natural Science Foundation of China (61502156); NSF Grants of Naval University of Engineering (HGDQNSQJJ15001); NSF Grants of Hubei Province (2014CFB189).

Biography: Ai Xiaochuan (1978–), female, born at Nanjing, Jiangsu, lector, major in number theory and cryptography.

Corresponding author: Chen Hua.

Till now, many improvements for (1.2) were made by Loxton, Vaughan and Smith [5, 6, 11]. Carlitz [7, 8] studied the computation problem of the two-term exponential $C(m,n,k;p)$ over finite fields and obtained the computational formulas for $k=3$ and $k=p+1$. As to the two-term exponential sums with Dirichlet character $C(m,n,k,\chi,q)=\sum\limits_{a=1}^{q}{}'\chi(a)e(\frac{ma^k+na}{q})$, Xu [13], Liu [3], Chen [14, 15], Ai [16] and Calderon [1] also acquired a lot of research results. More, about the three-term exponential sums, there were also some interesting results [17–19].

Though the single value of $C(m,n,k;q)$ is irregular, the high power means that value of $C(m,n,k;q)$ owns graceful arithmetical properties and it in turn becomes an interesting focus for many attentions. In 2010, Liu [4] acquired the computational formula of the fourth mean value, i.e., when p is an odd prime with $(n,p)=1$, then

$$\sum_{m=1}^{p}{}'|C(m,n,k;p)|^4=\begin{cases}(p-1)^4+p-2, & \text{if} \quad k=1;\\ p^3-p^2-7p-1-(-1)^{(p-1)/2}\cdot 2p, & \text{if} \quad k=2;\\ 2p^3-3p^2-3p-1, & \text{if} \quad k>0 \quad \text{and} \quad k\equiv -1(\mathrm{mod}p-1).\end{cases}$$

In 2011, Wang, Zhang [12] studied the computation problem of the fourth moment of two-term mixed exponential sums with elementary algebraic method. They proved that when p is a prime and $(n,p)=1$, then

$$\sum_{m=1}^{p}|C(m,n,2;p)|^4=\begin{cases}p(p^2-p-9), & \text{if} \quad p\equiv 1(\mathrm{mod}4);\\ p(p^2-p-5), & \text{if} \quad p\equiv 3(\mathrm{mod}4).\end{cases}$$

When p is a prime, $(n,p)=1$ and $(3,p-1)=1$, then

$$\sum_{m=1}^{p}|C(m,n,3;p)|^4=2p^3-3p^2-3p.$$

Unfortunately, though Liu, Wang got the explicit formulas of $\sum\limits_{m=1}^{p}|C(m,n,k;p)|^4$ with $k\geq 1, k=-1,1,2,3\ (\mathrm{mod}\,(p-1))$, the result under the condition $k\geq 1, k\equiv 5\ (\mathrm{mod}\,(p-1))$ was not solved. In this paper, this computation problem will be solved and the explicit formulas will be given. Moreover we shall give a transform formula and a lower bound formula for the fourth moment of two-term exponential sums. The main results are the following two theorems.

Theorem 1.1 Let p be a prime with $p\geq 5$, $(5,\ p-1)=1$, n be an integer with $(n,p)=1$, then for $k\geq 1, k\equiv 5\ (\mathrm{mod}(p-1))$, we have

$$\sum_{m=1}^{p}|C(m,n,k;p)|^4=\begin{cases}3p^3-8p^2-3p, & p\equiv 5\ (\mathrm{mod}12);\\ 3p^3-16p^2-3p, & p\equiv 1\ (\mathrm{mod}12);\\ 3p^3-10p^2-3p, & p\equiv -5\ (\mathrm{mod}12);\\ 3p^3-2p^2-3p, & p\equiv -1\ (\mathrm{mod}12).\end{cases}$$

Theorem 1.2 Let p be a prime with $p \geq 3$, $(k, p-1) = 1$, n be an integer with $(n, p) = 1$, then we have

$$\sum_{m=1}^{p} |C(m, n, k; p)|^4 \geq p(2p^2 - 3p - 3).$$

2 Preliminaries

To prove the main results, necessary lemmas are listed and proved as below.

Lemma 2.1 For arbitrary integers a, b, c, let p be an odd prime with $(a, p) = 1$ and denote N_1 as the number of the solutions of the congruence equation $ax^2+bx+c \equiv 0 \pmod{p}$, then

$$N_1 = 1 + \left(\frac{b^2 - 4ac}{p}\right).$$

Proof From Theorem 3.5.1 in ref. [10], we immediately get the result.

Lemma 2.2 Let p be an odd prime, N_2 denote the number of the solutions of the congruence equation $c^2 - c + 1 \equiv 0 \pmod{p}$, then

$$N_2 = \begin{cases} 2, & p \equiv 1, -5 \pmod{12}; \\ 0, & p \equiv 5, -1 \pmod{12}. \end{cases}$$

And if $p \equiv 1, -5 \pmod{12}, 1, p$ are not solutions.

Proof Since $(1, p) = 1$, by Lemma 2.1, we have

$$N_2 = 1 + \left(\frac{-3}{p}\right) = 1 + \left(\frac{p}{3}\right).$$

If $p \equiv 1, -5 \pmod{12}$, then $\left(\frac{p}{3}\right) = 1$;
If $p \equiv -1, 5 \pmod{12}$, then $\left(\frac{p}{3}\right) = -1$.
In conclusion, we have

$$N_2 = 1 + \left(\frac{p}{3}\right) = \begin{cases} 2, & p \equiv 1, -5 \pmod{12}; \\ 0, & p \equiv 5, -1 \pmod{12}. \end{cases}$$

And straight forward calculation shows that $1, p$ are not solutions.

Lemma 2.3 Let p be an odd prime, $a^2 - 4b \not\equiv 0 \pmod{p}$, then $\sum\limits_{x=1}^{p} \left(\frac{x^2+ax+b}{p}\right) = -1$, substituting 0 for the term in the formula with $p \mid x^2 + ax + b$.

Proof See Theorem 7.8.2 in ref. [10].

Lemma 2.4 Let p be an odd prime, k be an odd positive integer and $N_{k,p}$ denote the number of the solutions of the congruence equation

$$(a^k - 1)(c - 1)^k \equiv (c^k - 1)(a - 1)^k \pmod{p}, \tag{2.1}$$

where a, c are integers with $2 \leq a, c \leq p - 1$, then we have $N_{k,p} \geq 2p - 5$.

Proof It is obviously to show that $a \equiv c(\mathrm{mod}\ p)$ is fit for equation (2.1), now we consider the case $c \equiv \overline{a}(\mathrm{mod}\ p)$.

After substituting $c \equiv \overline{a}(\mathrm{mod}\ p)$ into the left part of formula (2.1), we have

$$(a^k - 1)(\overline{a} - 1)^k \equiv (a^k - 1)\overline{a}^k(1 - a)^k(\mathrm{mod}\ p).$$

Again, $c \equiv \overline{a}(\mathrm{mod}\ p)$ is substituted into the right part of (2.1). Since k is an odd integer, then

$$(\overline{a}^k - 1)(a - 1)^k \equiv \overline{a}^k(1 - a^k)(a - 1)^k \equiv (a^k - 1)\overline{a}^k(1 - a)^k(\mathrm{mod}\ p).$$

Therefore

$$(a^k - 1)(\overline{a} - 1)^k \equiv (\overline{a}^k - 1)(a - 1)^k(\mathrm{mod}\ p).$$

So $c \equiv \overline{a}(\mathrm{mod}\ p)$ is also fit for equation (2.1).

Moreover $a \equiv c(\mathrm{mod}\ p)$ and $a \equiv \overline{c}(\mathrm{mod}\ p)$ have the same solution $(a, c) = (p-1, p-1)$. Hence $N_{k,p} \geq 2p - 5$.

Lemma 2.5 Let p be a prime with $p > 3$ and N_3 denote the number of the solutions of the congruence equation

$$(c^2 - c + 1)a^2 - (c^2 + 1)a + (c^2 - c + 1) \equiv 0\ (\mathrm{mod}\ p), \tag{2.2}$$

where a, c are integers with $2 \leq a, c \leq p - 1$, then we have

$$N_3 = \begin{cases} p - 1, & p \equiv 5\ (\mathrm{mod}12); \\ p - 9, & p \equiv 1\ (\mathrm{mod}12); \\ p - 7, & p \equiv -5\ (\mathrm{mod}12); \\ p + 1, & p \equiv -1\ (\mathrm{mod}12). \end{cases}$$

Proof Case 1 For a fixed $c, 2 \leq c \leq p-1$, if $c^2 - c + 1 \not\equiv 0(\mathrm{mod}\ p)$, from Lemma 2.1, the number of the solutions of equation (2.2) is

$$\begin{aligned} & 1 + \left(\frac{(c^2+1)^2 - 4(c^2 - c + 1)^2}{p}\right) = 1 + \left(\frac{-c^2 + 2c - 1}{p}\right)\left(\frac{3c^2 - 2c + 3}{p}\right) \\ = \ & 1 + \left(\frac{-(c-1)^2}{p}\right)\left(\frac{3}{p}\right)\left(\frac{c^2 - 2 \cdot \overline{3} + 1}{p}\right) = 1 + \left(\frac{-3}{p}\right)\left(\frac{c^2 - 2 \cdot \overline{3} + 1}{p}\right), \end{aligned}$$

where $\overline{3}$ satisfies $3 \cdot \overline{3} \equiv 1\ (\mathrm{mod}\ p)$. If $a \equiv 1\ (\mathrm{mod}\ p)$ satisfies equation (2.2), then $c \equiv 1(\mathrm{mod}\ p)$; If $a \equiv 0\ (\mathrm{mod}\ p)$ satisfies equation (2.2), then $c^2 - c + 1 \equiv 0\ (\mathrm{mod}\ p)$, that contradicts.

Case 2 For a fixed $c, 2 \leq c \leq p - 1$, if $c^2 - c + 1 \equiv 0(\mathrm{mod}\ p)$, then equation (2.2) is $(c^2 + 1)a \equiv 0(\mathrm{mod}\ p)$, namely $ca \equiv 0(\mathrm{mod}\ p)$, therefore congruence equation (2.2) has no

solution. So we have

$$\begin{aligned}
N_3 &= \sum_{\substack{c=2 \\ c^2-c+1 \not\equiv 0 (\mathrm{mod}\ p)}}^{p-1} \left[1+\left(\frac{(c^2+1)^2-4(c^2-c+1)^2}{p}\right)\right] \\
&= \sum_{c=2}^{p-1} \left[1+\left(\frac{(c^2+1)^2-4(c^2-c+1)^2}{p}\right)\right] \\
&\quad - \sum_{\substack{c=2 \\ c^2-c+1 \equiv 0 (\mathrm{mod}\ p)}}^{p-1} \left[1+\left(\frac{(c^2+1)^2-4(c^2-c+1)^2}{p}\right)\right] \\
&= A-B. \\
A &= \sum_{c=2}^{p-1} \left[1+\left(\frac{-c^2+2c-1}{p}\right)\left(\frac{3c^2-2c+3}{p}\right)\right] \\
&= \sum_{c=2}^{p-1} \left[1+\left(\frac{-3}{p}\right)\left(\frac{c^2-2\cdot\overline{3}c+1}{p}\right)\right] \\
&= p-2+\left(\frac{-3}{p}\right)\cdot\sum_{c=2}^{p-1}\left(\frac{c^2-2\cdot\overline{3}c+1}{p}\right) \\
&= p-2+\left(\frac{-3}{p}\right)\cdot\sum_{c=1}^{p}\left[\left(\frac{c^2-2\cdot\overline{3}c+1}{p}\right)-\left(\frac{3}{p}\right)-1\right].
\end{aligned}$$

By using Lemma 2.3, we have

$$A = p-2+\left(\frac{-3}{p}\right)\cdot\left[-2-\left(\frac{3}{p}\right)\right] = p-2+\left(\frac{-1}{p}\right)-2\left(\frac{-3}{p}\right).$$

Now we compute B, from Lemma 2.2, we have

$$\begin{aligned}
B &= \sum_{\substack{c=2 \\ c^2-c+1 \equiv 0\ (\mathrm{mod}\ p)}}^{p-1} \left[1+\left(\frac{(c^2+1)^2}{p}\right)\right] \\
&= \sum_{\substack{c=2 \\ c^2-c+1 \equiv 0\ (\mathrm{mod}\ p)}}^{p-1} \left[1+\left(\frac{c^2}{p}\right)\right] = 2\cdot \sum_{\substack{c=2 \\ c^2-c+1 \equiv 0\ (\mathrm{mod}\ p)}}^{p-1} 1 \\
&= 2\cdot N_2,
\end{aligned}$$

where $N_2 = \begin{cases} 2, & p \equiv 1, -5\ (\mathrm{mod}12); \\ 0, & p \equiv 5, -1\ (\mathrm{mod}12). \end{cases}$ Therefore

$$N_3 = p-2-\left(\frac{-1}{p}\right)-2\left(\frac{-3}{p}\right)-2\cdot N_2.$$

If $p \equiv 5(\mathrm{mod}12)$, then $\left(\frac{-1}{p}\right) = 1$, $\left(\frac{-3}{p}\right) = -1$, therefore $N_3 = p - 1$.
If $p \equiv 1(\mathrm{mod}12)$, then $\left(\frac{-1}{p}\right) = 1$, $\left(\frac{-3}{p}\right) = 1$, therefore $N_3 = p - 9$.
If $p \equiv -5(\mathrm{mod}12)$, then $\left(\frac{-1}{p}\right) = -1$, $\left(\frac{-3}{p}\right) = 1$, therefore $N_3 = p - 7$.
If $p \equiv -1(\mathrm{mod}12)$, then $\left(\frac{-1}{p}\right) = -1$, $\left(\frac{-3}{p}\right) = -1$, therefore $N_3 = p + 1$.
In conclusion, we have

$$N_3 = \begin{cases} p-1, & p \equiv 5 \,(\mathrm{mod}12); \\ p-9, & p \equiv 1 \,(\mathrm{mod}12); \\ p-7, & p \equiv -5 \,(\mathrm{mod}12); \\ p+1, & p \equiv -1 \,(\mathrm{mod}12). \end{cases}$$

Lemma 2.6 Let p be a prime, $p > 5$ and $N_{5,p}$ denote the number of the solutions of the congruence equation

$$(a^5 - 1)(c - 1)^5 \equiv (c^5 - 1)(a - 1)^5 \,(\mathrm{mod}\ p), \tag{2.3}$$

where a, c are integers with $2 \le a, c \le p - 1$, then we have

$$N_{5,p} = \begin{cases} 3p-10, & p \equiv 5 \,(\mathrm{mod}12); \\ 3p-18, & p \equiv 1 \,(\mathrm{mod}12); \\ 3p-12, & p \equiv -5 \,(\mathrm{mod}12); \\ 3p-4, & p \equiv -1 \,(\mathrm{mod}12). \end{cases}$$

Proof By using factorization method, we know that equation (2.3) equivalents to

$$5(c-1)(a-1)(a-c)(ac-1)[(c^2-c+1)a^2-(c^2+1)a+(c^2-c+1)] \equiv 0 \,(\mathrm{mod}\ p).$$

Noting that p is a prime with $p > 5$ and $2 \le a, c \le p - 1$, we have

$$(a-c)(ac-1)[(c^2-c+1)a^2-(c^2+1)a+(c^2-c+1)] \equiv 0 \,(\mathrm{mod}\ p).$$

Let

$$\begin{aligned} S_1 &= \{(a,c) | a - c \equiv 0 \,(\mathrm{mod}\ p)\}, \\ S_2 &= \{(a,c) | ac \equiv 1 \,(\mathrm{mod}\ p)\}, \\ S_3 &= \{(a,c) | (c^2-c+1)a^2-(c^2+1)a+(c^2-c+1) \equiv 0 \,(\mathrm{mod}\ p)\}, \end{aligned}$$

then

$$N_{5,p} = |S_1 \cup S_2 \cup S_3| = |S_1| + |S_2| + |S_3| - |S_1 \cap S_2| - |S_1 \cap S_3| - |S_2 \cap S_3| + |S_1 \cap S_2 \cap S_3|,$$

where $|\quad|$ denotes the number of the elements of the set.

(a) It is obviously that $S_1 \cap S_2 = \{(p-1, p-1)\}$ and thus $|S_1 \cap S_2| = 1$.

(b) If $(a,c) \in S_1 \cap S_3$, then

$$(c^2+1)(c-1)^2 \equiv 0 \,(\mathrm{mod}\ p).$$

Since $c \not\equiv 1 \,(\mathrm{mod}\ p)$, we have

$$c^2 \equiv -1 (\mathrm{mod}\ p). \tag{2.4}$$

If $p \equiv 1 \,(\mathrm{mod}4)$, then $\left(\frac{-1}{p}\right) = 1$, so equation (2.4) has two solutions and obviously $c \equiv 0, 1, p-1 \,(\mathrm{mod}\ p)$ are not solutions. Therefore

$$|S_1 \cap S_3| = 2, |S_1 \cap S_2 \cap S_3| = 0.$$

If $p \equiv -1 \,(\mathrm{mod}4)$, then $\left(\frac{-1}{p}\right) = -1$, so equation (2.4) has no solution. Therefore

$$|S_1 \cap S_3| = 0, |S_1 \cap S_2 \cap S_3| = 0.$$

(c) If $(a,c) \in S_2 \cap S_3$, then we substitute $a \equiv \overline{c} \,(\mathrm{mod}\ p)$ into the equation

$$(c^2-c+1)a^2 - (c^2+1)a + (c^2-c+1) \equiv 0 \,(\mathrm{mod}\ p),$$

then

$$(c^2-c+1)(\overline{c})^2 - (c^2+1)\overline{c} + (c^2-c+1) \equiv 0 \,(\mathrm{mod}\ p).$$

Thus

$$(c^2-c+1)c^2 - (c^2+1)c + (c^2-c+1) \equiv 0 \,(\mathrm{mod}\ p),$$

namely,

$$(c^2+1)(c-1)^2 \equiv 0 \,(\mathrm{mod}\ p).$$

Now we can see that the case is similar to case (b). Therefore we have if $p \equiv 1 \,(\mathrm{mod}\,4)$, then $|S_2 \cap S_3| = 2$; if $p \equiv -1 \,(\mathrm{mod}4)$, then $|S_2 \cap S_3| = 0$. So

$$N_{5,p} = 2p - 5 + |S_3| - |S_1 \cap S_3| - |S_2 \cap S_3|\,.$$

From Lemma 2.5, we have

$$S_3 = \begin{cases} p-1, & p \equiv 5 \,(\mathrm{mod}12); \\ p-9, & p \equiv 1 \,(\mathrm{mod}12); \\ p-7, & p \equiv -5 \,(\mathrm{mod}12); \\ p+1, & p \equiv -1 \,(\mathrm{mod}12). \end{cases}$$

Then

$$N_{5,p} = \begin{cases} 3p-10, & p \equiv 5 \,(\mathrm{mod}12); \\ 3p-18, & p \equiv 1 \,(\mathrm{mod}12); \\ 3p-12, & p \equiv -5 \,(\mathrm{mod}12); \\ 3p-4, & p \equiv -1 \,(\mathrm{mod}12). \end{cases}$$

Lemma 2.7 Let p be an odd prime with $(n,p)=1$ and $(k,p-1)=1$, then we have

$$\sum_{m=1}^{p}|C(m,n,k;p)|^4=2p^2-3p+p^2\cdot N_{k,p}.$$

Proof For integer r satisfying $(r,p)=1$, we have $(\overline{r},p)=1$, where $r\overline{r}\equiv 1 \pmod p$. Thus we have

$$\begin{aligned}\sum_{m=1}^{p}|C(m,n,k;p)|^4 &= \sum_{m=1}^{p}\left|{\sum_{a=1}^{p}}'e(\frac{ma^k+na}{p})\right|^4=\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1}e(\frac{m\overline{r}^ka^k+na}{p})\right|^4\\ &= \frac{1}{p-1}\sum_{r=1}^{p-1}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1}e(\frac{m\overline{r}^k(ra)^k+n(ra)}{p})\right|^4\\ &= \frac{1}{p-1}\sum_{r=1}^{p-1}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1}e(\frac{ma^k+n(ra)}{p})\right|^4\\ &= \frac{1}{p-1}\sum_{r=1}^{p}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1}e(\frac{ma^k+n(ra)}{p})\right|^4-\frac{1}{p-1}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1}e(\frac{ma^k}{p})\right|^4\\ &= T_1-T_2.\end{aligned}$$

Noting that $(k,p-1)=1$, then

$$\begin{aligned}T_2 &= \frac{1}{p-1}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1}e(\frac{ma^k}{p})\right|^4=\frac{1}{p-1}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1}e(\frac{ma}{p})\right|^4\\ &= \frac{1}{p-1}\left[(p-1)^4+\sum_{m=1}^{p-1}\left|\sum_{a=1}^{p-1}e(\frac{ma}{p})\right|^4\right]=(p-1)^3+1.\\ T_1 &= \frac{1}{p-1}\sum_{r=1}^{p}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}e(\frac{m(a^k-b^k)+nr(a-b)}{p})\right|^2\\ &= \frac{1}{p-1}\sum_{r=1}^{p}\sum_{m=1}^{p}\left|p-1+\sum_{a=2}^{p-1}\sum_{b=1}^{p-1}e(\frac{mb^k(a^k-1)+nrb(a-1)}{p})\right|^2\\ &= \frac{1}{p-1}\sum_{r=1}^{p}\sum_{m=1}^{p}\left|p-1+\sum_{a=2}^{p-1}\sum_{b=1}^{p-1}e(\frac{mb^k(\overline{a-1})^k(a^k-1)+nrb}{p})\right|^2\\ &= \frac{1}{p-1}\sum_{r=1}^{p}\sum_{m=1}^{p}\left[p-1+\sum_{a=2}^{p-1}\sum_{b=1}^{p-1}e(\frac{mb^k(\overline{a-1})^k(a^k-1)+nrb}{p})\right]\\ &\quad\cdot\left[p-1+\sum_{c=2}^{p-1}\sum_{d=1}^{p-1}e(\frac{-md^k(\overline{c-1})^k(c^k-1)-nrd}{p})\right]\end{aligned}$$

$$\begin{aligned}
&= (p-1)p^2+\sum_{r=1}^{p}\sum_{m=1}^{p}\sum_{a=2}^{p-1}\sum_{b=1}^{p-1}e(\frac{m(b(\overline{a-1}))^k(a^k-1)+nrb}{p})\\
&\quad+\sum_{r=1}^{p}\sum_{m=1}^{p}\sum_{c=2}^{p-1}\sum_{d=1}^{p-1}e(\frac{-m(d(\overline{c-1}))^k(c^k-1)-nrd}{p})\\
&\quad+\frac{1}{p-1}\sum_{r=1}^{p}\sum_{m=1}^{p}\sum_{a=2}^{p-1}\sum_{b=1}^{p-1}\sum_{c=2}^{p-1}\sum_{d=1}^{p-1}e(\frac{m\left[(b(\overline{a-1}))^k(a^k-1)-(d(\overline{c-1}))^k(c^k-1)\right]+nr(b-d)}{p})\\
&= (p-1)p^2+T_{11}+T_{12}+T_{13}.\\
T_{11} &= \sum_{r=1}^{p}\sum_{m=1}^{p}\sum_{a=2}^{p-1}\sum_{b=1}^{p-1}e(\frac{m(b(\overline{a-1}))^k(a^k-1)+nrb}{p})\\
&= \sum_{m=1}^{p}\sum_{a=2}^{p-1}\sum_{b=1}^{p-1}e(\frac{m(b(\overline{a-1}))^k(a^k-1)}{p})\sum_{r=1}^{p}e(\frac{nrb}{p}).
\end{aligned}$$

With the condition $(n,p)=1$ and from the trigonometric identity,

$$\sum_{a=1}^{m}e(\frac{na}{m})=\begin{cases} m, & m\mid n,\\ 0, & m\nmid n.\end{cases}$$

We have $\sum\limits_{r=1}^{p}e(\frac{nrb}{p})=0$, therefore $T_{11}=0$. Similarly, $T_{12}=0$,

$$\begin{aligned}
T_{13} &= \frac{1}{p-1}\sum_{r=1}^{p}\sum_{m=1}^{p}\sum_{a=2}^{p-1}\sum_{b=1}^{p-1}\sum_{c=2}^{p-1}\sum_{d=1}^{p-1}e(\frac{m\left[(b(\overline{a-1}))^k(a^k-1)-(d(\overline{c-1}))^k(c^k-1)\right]+nr(b-d)}{p})\\
&= \frac{1}{p-1}\sum_{m=1}^{p}\sum_{a=2}^{p-1}\sum_{b=1}^{p-1}\sum_{c=2}^{p-1}\sum_{d=1}^{p-1}e(\frac{m\left[(b(\overline{a-1}))^k(a^k-1)-(d(\overline{c-1}))^k(c^k-1)\right]}{p})\sum_{r=1}^{p}e(\frac{nr(b-d)}{p})\\
&= \frac{p}{p-1}\sum_{\substack{m=1\\ b\equiv d\pmod p}}^{p}\sum_{a=2}^{p-1}\sum_{b=1}^{p-1}\sum_{c=2}^{p-1}\sum_{d=1}^{p-1}e(\frac{m\left[(b(\overline{a-1}))^k(a^k-1)-(d(\overline{c-1}))^k(c^k-1)\right]}{p})\\
&= \frac{p}{p-1}\sum_{m=1}^{p}\sum_{a=2}^{p-1}\sum_{b=1}^{p-1}\sum_{c=2}^{p-1}e(\frac{mb\left[(\overline{a-1})^k(a^k-1)-(\overline{c-1})^k(c^k-1)\right]}{p})\\
&= \frac{p}{p-1}\sum_{c=2}^{p-1}\sum_{a=2}^{p-1}\sum_{b=1}^{p-1}\sum_{m=1}^{p}e(\frac{mb\left[(\overline{a-1})^k(a^k-1)-(\overline{c-1})^k(c^k-1)\right]}{p})\\
&= p^2\cdot\sum_{\substack{a=2\\ (\overline{a-1})^k(a^k-1)-(\overline{c-1})^k(c^k-1)\equiv 0\pmod p}}^{p-1}\sum_{c=2}^{p-1}1\\
&= p^2\cdot\sum_{\substack{a=2\\ (a^k-1)(c-1)^k\equiv(c^k-1)(a-1)^k\pmod p}}^{p-1}\sum_{c=2}^{p-1}1\\
&= p^2\cdot N_{k,p}.
\end{aligned}$$

So

$$\sum_{m=1}^{p}|C(m,n,k;p)|^4=2p^2-3p+p^2\cdot N_{k,p}.$$

Thus all of the lemmas are shown. Besides, the result of Lemma 2.7 shows that the difficulty of calculating $\sum_{m=1}^{p} |C(m,n,k;p)|^4$ is mainly stemmed from computing exactly number of the solutions of high power congruence equation.

3 Proof of the Theorems

First we prove Theorem 1.1.

Proof By Lemma 2.7, we have

$$\sum_{m=1}^{p} |C(m,n,k;p)|^4 = \sum_{m=1}^{p} |C(m,n,5;p)|^4 = 2p^2 - 3p + p^2 \cdot N_{5,p}.$$

From Lemma 2.6, we have

$$N_{5,p} = \begin{cases} 3p-10, & p \equiv 5 \pmod{12}; \\ 3p-18, & p \equiv 1 \pmod{12}; \\ 3p-12, & p \equiv -5 \pmod{12}; \\ 3p-4, & p \equiv -1 \pmod{12}. \end{cases}$$

Therefore

$$\sum_{m=1}^{p} |C(m,n,k;p)|^4 = \begin{cases} 3p^3-8p^2-3p, & p \equiv 5 \pmod{12}; \\ 3p^3-16p^2-3p, & p \equiv 1 \pmod{12}; \\ 3p^3-10p^2-3p, & p \equiv -5 \pmod{12}; \\ 3p^3-2p^2-3p, & p \equiv -1 \pmod{12}. \end{cases}$$

This proves Theorem 1.1.

Finally we complete the proof of Theorem 1.2.

Proof By Lemma 2.7 and Lemma 2.4, we have

$$\begin{aligned} \sum_{m=1}^{p} |C(m,n,k;p)|^4 &= 2p^2 - 3p + p^2 \cdot N_{k,p} \\ &\geq 2p^2 - 3p + p^2 \cdot (2p-5) = p(2p^2-3p-3). \end{aligned}$$

References

[1] Calderon C, Develasco M J, Zarate M J. An explicit formula for the fourth moment of certain exponential sums[J]. Acta Math. Hungar, 2011, 130(3): 203–222.

[2] Darvenport H, Heibronn H. On an exponential sum[J]. Proc. London Math. Soc., 1936, 41: 49–53.

[3] Liu H N. Mean value of mixed exponential sums[J]. Proc. Amer. Math. Soc., 2008, 136(4): 1193–1203.

[4] Liu H N. Mean value of some exponential sums and applications to Kloosterman sums[J]. J. Math. Anal. Appl., 2010, 361(4): 205–223.

[5] Loxton J H, Smith R A. On Hua's estimate for exponential sums[J]. J. London Math. Soc., 1982, 26(2): 15–20.

[6] Loxton J H, Vaughan R C. The estimate for complete exponential sums[J]. Canada Math. Bull., 1995, 26(4): 442–454.

[7] Carlitz L. Explicit evaluation of certain exponential sums[J]. Math. Scand., 1979, 44: 5–16.

[8] Carlitz L. Evaluation of some exponential sums over a finite field[J]. Math. Nachr., 1980, 96: 319–339.

[9] Hua L K. On exponential sums[M]. Peking, N.S.: Sci. Record, 1957.

[10] Hua L K. Introduction to number theory[M]. Beijing: Sci. Press, 1979.

[11] Smith R A. On n-dimensional Kloosterman sums[J]. J. Number Theory, 1979, 11: 324–343.

[12] Wang T T, Zhang W P. Mean value of the mixed fourth and sixth exponential sums[J]. China Sci., 2011, 41(3): 265–270.

[13] Xu Z F, Zhang T P, Zhang W P. On the mean value of the two-term exponential sums with Dirichlet characters[J]. J. Number Theory, 2007, 123(2): 352–362.

[14] Chen H, Chen J H, Cai G X, Ai X C, Zhang S L. Explicit formulas for the fourth moment of mixed exponential sums[J]. J. Number Theory, 2013, 133(5): 1484–1491.

[15] Chen H, Ai X C, Cai G X. A note on mean value of mixed exponential sums[J]. J. Number Theory, 2014, 144(11): 234–243.

[16] Ai X C, Chen J H, Chen H, Zhang S L. Explicit formulas for the fourth moment of certain two-term exponential sums[J]. J. Comp. Model. New Tech., 2014, 18(12A): 232–239.

[17] Ai X C, Chen J H, Chen H, Zhang S L. Explicit formulas for the fourth moment of three-term exponential sums[A]. 2014 International Joint Conference on Applied Mathematics, Statistics and Public Administration (IJAMSPA 2014)[C]. Changsha: ISBN: 978-1-60595-187-4.

[18] Ai X C, Chen J H, Zhang S L, Chen H. Researching the relation between the three-term exponential sums and the system of the congruence equations[J]. J. Math., 2013, 33(3): 535–540.

[19] Ai X C, Chen J H, Chen H, Zhang S L. Explicit formulas for the mean value of high gauss sums. J. Math., 2015, 35(4): 941–944.

二项指数和四次混合均值的计算

艾小川[1], 陈 华[2], 张四兰[3]

(1. 海军工程大学理学院应用数学系, 湖北 武汉 430033)

(2. 湖北工业大学理学院, 湖北 武汉 430068)

(3. 华中农业大学理学院, 湖北 武汉 430070)

摘要: 本文研究了二项指数和四次均值的计算问题. 利用初等数论及代数数论的方法获得了一个精确的计算公式以及一个转换公式, 推广了已有的结果, 揭示了均值计算与同余方程组的本质联系.

关键词: 二项指数和; 混合均值; 四次均值; 转换公式

MR(2010)**主题分类号**: 11T23; 11T24 **中图分类号**: O156.2