Vol. 37 (2017)
No. 1

数 学 杂 志
J. of Math. (PRC)

三项指数和四次均值的精确计算公式 (2)

艾小川 [1], 陈 华 [2], 张四兰 [3]
(1. 海军工程大学理学院, 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: 本文进一步深入研究了三项指数和四次均值的计算问题. 运用指数和的相关性质并结合求解同余方程组的方法与技巧, 利用两种不同的方法获得了两个精确的均值计算公式, 揭示了三项指数和的计算与同余方程组解的个数之间的本质联系, 推广了已有的结果.

关 键 词: 三项指数和; 四次均值; 转换公式; 同余方程组
MR(2010) **主题分类号:** 11T23; 11T24 **中 图 分 类 号:** 0156.4
文 献 标 识 码: A **文 章 编 号:** 0255-7797(2017)01-0177-08

1 引言

指数和与著名的华林问题有着密切的联系, 它在华林问题的主项研究中起着重要的作用. 许多著名的学者如华罗庚、Weil、高斯等对指数和的上界估计做出了重要的贡献 [1−6]. 近些年来, 指数和高次均值的计算成了这一领域的热点, 相关研究成果丰硕 [7−11,13−17].

设 q, m, s, n, k, t 为整数, 且 $q \geq 3$, 定义二项指数和与三项指数和如下:

$$\sum_{a=1}^{q}{}'e(\frac{ma^k+na}{q}),$$
$$\sum_{a=1}^{q}{}'e(\frac{ma^k+sa^t+na}{q}),$$

其中 $e(x)=e^{2\pi ix}$, $\sum\limits_{a=1}^{q}{}'$ 表示对所有满足 $(a,q)=1$ 的整数 a 求和.

国内外众多学者对于二项指数和的各种性质做了深入细致的研究, 取得了众多的研究成果 [7−11,16,17]. 但是关于三项指数和的各类性质, 国内外的相关研究尚不多见.

1972 年, Mordel[12] 利用三项指数和成功的研究 $\bmod p$ 剩余类的有理函数表示.

2012 年, 陈华等人 [13] 研究了带 Dirichlet 特征的三项指数和四次均值的计算公式, 并给出了 $\sum\limits_{t=1}^{q}{}'\sum\limits_{m=1}^{q}\sum\limits_{\chi \bmod q}|\sum\limits_{a=1}^{q}{}'\chi(a)e(\frac{ma^k+ta^2+na}{q})|^4$ 的精确计算公式.

*收稿日期: 2014-06-27 接收日期: 2014-11-26
基金项目:国家自然科学基金 (NSFC61502156); 海军工程大学自然科学基金 (HGDQNSQJJ15001); 湖北省自然科学基金 (2014CFB189); 湖北工业大学博士启动基金 (BSQD13051).
作者简介: 艾小川 (1978–), 女, 江苏南京, 讲师, 主要研究方向: 数论与密码学.
通讯作者: 陈华.

2014 年, 论文 [14] 给出了三项指数和的四次均值

$$\sum_{s=1}^{p}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1}e(\frac{ma^k+sa^t+na}{p})\right|^4$$

在 $k=2t,(t,p-1)=1,2$ 时的精确计算公式, 主要结果如下:

命题 1.1 设 p 为素数, 则对任意固定的满足条件 $(n,p)=1$ 的正整数 n, 有

$$\sum_{s=1}^{p}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1}e(\frac{ma^{2t}+sa^t+na}{p})\right|^4=p^2(2p^2-5p+3),(t,p-1)=1;$$

$$\sum_{s=1}^{p}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1}e(\frac{ma^{2t}+sa^t+na}{p})\right|^4=p^2(2p^2-11p+16),(t,p-1)=2.$$

本文将进一步深入讨论三项指数和四次均值的计算问题, 在命题 1.1 的条件下, 给出在 $(t,p-1)=3,4$ 时的精确计算公式, 本文主要结果见定理 1.1. 此外, 本文还将给出命题 1.1 和定理 1.1 的一个简化证明方法.

定理 1.1 设 p 为奇素数, 则对任意固定的满足条件 $(n,p)=1$ 的正整数 n, 有

$$\sum_{s=1}^{p}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1}e(\frac{ma^{2t}+sa^t+na}{p})\right|^4=p^2(2p^2-17p+45),(t,p-1)=3;$$

$$\sum_{s=1}^{p}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1}e(\frac{ma^{2t}+sa^t+na}{p})\right|^4=\begin{cases}p^2(2p^2-25p+96),p\nmid(-4)^{t/4}-1,\\ p^2(2p^2-29p+96),p\mid(-4)^{t/4}-1,\end{cases}\quad(t,p-1)=4.$$

2 引理和定理的证明

首先给出定理证明中需要用到的几个引理.

引理 2.1 设 $p\geq 3,t$ 是正整数, $(n,p)=1$, 则有

$$\sum_{s=1}^{p}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1}e(\frac{ma^{2t}+sa^t+na}{p})\right|^4=p^4-p^3+[M+(l-1)^2]p^3-l^2p^2(2p-2-l),$$

其中

$$l=(t,p-1),\ M=\sum_{\substack{a=2}}^{p-1}\sum_{c=2}^{p-1}1\quad.$$
$$\scriptstyle (a\bar{c})^t\equiv 1\,(\mathrm{mod}p)$$
$$\scriptstyle [(a-1)\overline{(c-1)}]^t\equiv 1\ (\mathrm{mod}\ p)$$
$$\scriptstyle c^t\not\equiv 1\ (\mathrm{mod}\ p)$$

证 参见文献 [14] 中的引理 3.

引理 2.2
$$\sum_{\substack{a=2}}^{p-1}\sum_{c=2}^{p-1}1=\begin{cases}p-2, & (t,p-1)=3;\\ p-1,p\nmid(-4)^{t/4}-1, & (t,p-1)=4;\\ p-5,p\mid(-4)^{t/4}-1, & (t,p-1)=4.\end{cases}$$
$$\scriptstyle (a\bar{c})^t\equiv 1\,(\mathrm{mod}p)$$
$$\scriptstyle [(a-1)\overline{(c-1)}]^t\equiv 1\ (\mathrm{mod}\ p)$$
$$\scriptstyle c^t\not\equiv 1\ (\mathrm{mod}\ p)$$

证 易见 $\sum\limits_{a=2}^{p-1}\sum\limits_{c=2}^{p-1}1$ 的值为如下同余方程组解的个数,

$$\begin{subarray}{c}(a\overline{c})^t\equiv 1\ (\mathrm{mod}p)\\ [(a-1)\overline{(c-1)}]^t\equiv 1\ (\mathrm{mod}\ p)\\ c^t\not\equiv 1\ (\mathrm{mod}\ p)\end{subarray}$$

$$\begin{cases} c^t\not\equiv 1\ (\mathrm{mod}p),\\ (a\overline{c})^t\equiv 1\ (\mathrm{mod}p),\\ [(a-1)\overline{(c-1)}]^t\equiv 1\ \ (\mathrm{mod}p),\end{cases}\tag{2.1}$$

其中 $2\le a,c\le p-1$.

情形 1 若 $(t,p-1)=3$, 则 $x^t\equiv 1\ (\mathrm{mod}p)$ 有 3 个解, 分别记为 $1,A,\overline{A}$, 其中 $\overline{A}\equiv A^2(\mathrm{mod}p), A^3\equiv 1\ (\mathrm{mod}p)$, 则 (2.1) 等价于如下方程组:

$$\begin{cases} c^t\not\equiv 1\ (\mathrm{mod}p),\\ a\equiv c, Ac, \overline{A}c\ (\mathrm{mod}p),\\ a-1\equiv (c-1), A(c-1), \overline{A}(c-1)\ \ (\mathrm{mod}p).\end{cases}$$

(1) 若 $\begin{cases} c^t\not\equiv 1\ (\mathrm{mod}p),\\ a\equiv c\ (\mathrm{mod}p),\\ a-1\equiv c-1\ (\mathrm{mod}p),\end{cases}$ 则 $\begin{cases} c^t\not\equiv 1\ (\mathrm{mod}p),\\ a\equiv c\ \ (\mathrm{mod}p),\end{cases}$ 满足 $c^t\equiv 1\ (\mathrm{mod}p)$ 的 c 有 $(t,p-1)=3$ 个, 此种情形下共有 $p-1-3=p-4$ 个解;

(2) 若 $\begin{cases} c^t\not\equiv 1\ (\mathrm{mod}p),\\ a\equiv c\ (\mathrm{mod}p),\\ a-1\equiv A(c-1)(\mathrm{mod}p)\end{cases}$ 或 $\begin{cases} c^t\not\equiv 1\ (\mathrm{mod}p),\\ a\equiv c\ (\mathrm{mod}p),\\ a-1\equiv \overline{A}(c-1)(\mathrm{mod}p),\end{cases}$ 则 $A,\overline{A}\equiv 1\ (\mathrm{mod}\ p)$, 与 $A,\overline{A}\not\equiv 1\ (\mathrm{mod}p)$ 矛盾, 无解;

(3) 若 $\begin{cases} c^t\not\equiv 1\ (\mathrm{mod}p),\\ a\equiv Ac\ (\mathrm{mod}p),\\ a-1\equiv (c-1)(\mathrm{mod}p)\end{cases}$ 或 $\begin{cases} c^t\not\equiv 1\ (\mathrm{mod}p),\\ a\equiv \overline{A}c\ (\mathrm{mod}p),\\ a-1\equiv (c-1)(\mathrm{mod}p),\end{cases}$ 则 $A,\overline{A}\equiv 1\ (\mathrm{mod}p)$, 与 $A,\overline{A}\not\equiv 1\ (\mathrm{mod}p)$ 矛盾, 无解;

(4) 若 $\begin{cases} c^t\not\equiv 1\ (\mathrm{mod}p),\\ a\equiv Ac\ (\mathrm{mod}p),\\ a-1\equiv A(c-1)(\mathrm{mod}p)\end{cases}$ 或 $\begin{cases} c^t\not\equiv 1\ (\mathrm{mod}p),\\ a\equiv \overline{A}c\ (\mathrm{mod}p),\\ a-1\equiv \overline{A}(c-1)(\mathrm{mod}p),\end{cases}$ 则 $A,\overline{A}\equiv 1\ (\mathrm{mod}\ p)$, 与 $A,\overline{A}\not\equiv 1\ (\mathrm{mod}p)$ 矛盾, 无解;

(5) 若 $\begin{cases} c^t\not\equiv 1\ (\mathrm{mod}p),\\ a\equiv \overline{A}c\ (\mathrm{mod}p),\\ a-1\equiv A(c-1)\ (\mathrm{mod}p),\end{cases}$ 则 $\begin{cases} c^t\not\equiv 1\ (\mathrm{mod}p),\\ c\equiv 1+A\ (\mathrm{mod}p),\end{cases}$ 由 $A^3\equiv 1\ (\mathrm{mod}\,p)$ 可得 $1+A+A^2\equiv 0(\mathrm{mod}\,p)$, 则 $1+A\equiv -A^2(\mathrm{mod}\,p), c^t\equiv (-A^2)^t\equiv (-1)^tA^{2t}\equiv -1\not\equiv 1\ (\mathrm{mod}\,p)$, 保留此解;

(6) 若 $\begin{cases} c^{2t}\not\equiv 1\ (\mathrm{mod}p),\\ a\equiv Ac\ (\mathrm{mod}p),\\ a-1\equiv \overline{A}(c-1)\ (\mathrm{mod}p),\end{cases}$ 则 $\begin{cases} c^t\not\equiv 1\ (\mathrm{mod}p),\\ c\equiv -A\ (\mathrm{mod}p),\end{cases}$ 同 (5) 的情形, 保留此解.

所以

$$M=p-2.$$

情形 2 若 $(t,p-1)=4$, 则 $x^t\equiv 1\,(\mathrm{mod}p)$ 有 4 个解, 分别记为 $\pm1,\pm A$, 其中 $A^2\equiv -1\,(\mathrm{mod}p)$ 所以 (2.1) 式等价于如下方程组:

$$\begin{cases} c^t\not\equiv 1 & (\mathrm{mod}p),\\ a\equiv \pm c;\pm cA & (\mathrm{mod}p),\\ a-1\equiv \pm(c-1);\pm A(c-1)(\mathrm{mod}p), \end{cases}$$

且易见 $-2\overline{(A-1)}\equiv A+1\,(\mathrm{mod}p), A^2\equiv -1\,(\mathrm{mod}p), \overline{A}\equiv -A\,(\mathrm{mod}p), A^4\equiv 1\,(\mathrm{mod}p)$.

(1) 若 $\begin{cases} c^t\not\equiv 1\,(\mathrm{mod}p),\\ a\equiv c\,(\mathrm{mod}p),\\ a-1\equiv c-1\,(\mathrm{mod}p), \end{cases}$ 则 $\begin{cases} c^t\not\equiv 1\,(\mathrm{mod}p),\\ a\equiv c(\mathrm{mod}p), \end{cases}$ 满足 $c^t\equiv 1\,(\mathrm{mod}p)$ 的 c 有 $(t,p-1)=4$ 个, 则此种情形下共有 $p-1-(t,p-1)=p-5$ 个解;

(2) 若 $\begin{cases} c^t\not\equiv 1\,(\mathrm{mod}p),\\ a\equiv -c\,(\mathrm{mod}p),\\ a-1\equiv c-1\,(\mathrm{mod}p), \end{cases}$ 此种情形无解;

(3) 若 $\begin{cases} c^t\not\equiv 1\,(\mathrm{mod}p),\\ a\equiv c\,(\mathrm{mod}p),\\ a-1\equiv -c+1\,(\mathrm{mod}p), \end{cases}$ 则 $\begin{cases} c^t\not\equiv 1\,(\mathrm{mod}p),\\ a\equiv c\equiv 1\,(\mathrm{mod}p), \end{cases}$ 此种情形无解;

(4) 若 $\begin{cases} c^t\not\equiv 1\,(\mathrm{mod}p),\\ a\equiv -c\,(\mathrm{mod}p),\\ a-1\equiv -c+1\,(\mathrm{mod}p), \end{cases}$ 此种情形无解;

(5) 若 $\begin{cases} c^t\not\equiv 1\,(\mathrm{mod}p),\\ a\equiv c\,(\mathrm{mod}p),\\ a-1\equiv \pm A(c-1)(\mathrm{mod}p), \end{cases}$ $\begin{cases} c^t\not\equiv 1\,(\mathrm{mod}p),\\ a\equiv \pm Ac\,(\mathrm{mod}p),\\ a-1\equiv c-1\,(\mathrm{mod}p), \end{cases}$

或 $\begin{cases} c^t\not\equiv 1\,(\mathrm{mod}p),\\ a\equiv \pm Ac\,(\mathrm{mod}p),\\ a-1\equiv \pm A(c-1)(\mathrm{mod}p), \end{cases}$ 则 $A\equiv\pm1\,(\mathrm{mod}p)$, 与 $A\not\equiv\pm1\,(\mathrm{mod}p)$ 矛盾, 无解;

(6) 若 $\begin{cases} c^t\not\equiv 1\,(\mathrm{mod}p),\\ a\equiv -c\,(\mathrm{mod}p),\\ a-1\equiv \pm A(c-1)(\mathrm{mod}p), \end{cases}$ 则 $\begin{cases} c^t\not\equiv 1\ \ (\mathrm{mod}p),\\ a\equiv \mp A\,(\mathrm{mod}p),\\ c\equiv \pm A\,(\mathrm{mod}p), \end{cases}$

此时 $c^t\equiv A^t\equiv 1\,(\mathrm{mod}p)$ 与条件 $c^t\not\equiv 1\,(\mathrm{mod}p)$ 矛盾, 无解;

(7) 若 $\begin{cases} c^t\not\equiv 1\,(\mathrm{mod}p),\\ a\equiv Ac\,(\mathrm{mod}p),\\ a-1\equiv -c+1\,(\mathrm{mod}p), \end{cases}$ 则 $\begin{cases} c^t\not\equiv 1\ \ (\mathrm{mod}p),\\ a\equiv A+1\,(\mathrm{mod}p),\\ c\equiv 1-A\,(\mathrm{mod}p), \end{cases}$

此时

$$c^t\equiv (c^4)^{t/4}\equiv[(1-A)^4]^{t/4}\equiv[(1-2A+A^2)^2]^{t/4}\equiv[(-2A)^2]^{t/4}\equiv[4A^2]^{t/4}\equiv(-4)^{t/4}(\ \mathrm{mod}\ p).$$

若 $p\nmid(-4)^{t/4}-1$, 则 $c^t\equiv(1-A)^t\equiv(-4)^{t/4}\not\equiv 1\,(\mathrm{mod}p)$, 此时 $(a,c)=(A+1,1-A)$ 是解.

若 $p\,|\,(-4)^{t/4}-1$, 则 $c^t\equiv(1-A)^t\equiv(-4)^{t/4}\equiv 1\,(\mathrm{mod}p)$, 此时 $(a,c)=(A+1,1-A)$ 不是解;

(8) 若 $\begin{cases} c^t \not\equiv 1\,(\mathrm{mod}p), \\ a \equiv -Ac\,(\mathrm{mod}p), \\ a-1 \equiv -c+1\,(\mathrm{mod}p), \end{cases}$ $\begin{cases} c^t \not\equiv 1\,(\mathrm{mod}p), \\ a \equiv -Ac\,(\mathrm{mod}p), \\ a-1 \equiv A(c-1)(\mathrm{mod}p), \end{cases}$

或 $\begin{cases} c^t \not\equiv 1\,(\mathrm{mod}p), \\ a \equiv Ac\,(\mathrm{mod}p), \\ a-1 \equiv -A(c-1)(\mathrm{mod}p), \end{cases}$ 这三种情形类同 (7).

所以

$$M = \begin{cases} p-1, p \nmid (-4)^{t/4}-1, \\ p-5, p \mid (-4)^{t/4}-1. \end{cases}$$

下面证明定理 1.1.

在引理 2.1 中令 $(t, p-1)=3$, 结合引理 2.2 可得

$$\begin{aligned} \sum_{s=1}^{p}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1} e(\frac{ma^{2t}+sa^t+na}{p})\right|^4 &= p^4-p^3+[M+(l-1)^2]p^3-l^2p^2(2p-2-l) \\ &= p^4-p^3+[p-2+(3-1)^2]p^3-3^2p^2(2p-2-3), \\ &= = p^2(2p^2-17p+45). \end{aligned}$$

类似的, 在引理 2.1 中令 $(t, p-1)=4$, 结合引理 2.2 可得

$$\sum_{s=1}^{p}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1} e(\frac{ma^{2t}+sa^t+na}{p})\right|^4 = \begin{cases} p^2(2p^2-25p+96), p \nmid (-4)^{t/4}-1, \\ p^2(2p^2-29p+96), p \mid (-4)^{t/4}-1 \end{cases} \quad (t, p-1)=4.$$

在命题 1.1 及定理 1.1 中令 $t=1,2,3,4$, 可得如下结论.

推论 2.1 设 p 为素数, 则对任意固定的满足条件 $(n,p)=1$ 的正整数 n , 有

$$\sum_{s=1}^{p}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1} e(\frac{ma^4+sa^2+na}{p})\right|^4 = p^2(2p^2-11p+16), p \geq 5.$$

$$\sum_{s=1}^{p}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1} e(\frac{ma^6+sa^3+na}{p})\right|^4 = \begin{cases} p^2(2p^2-17p+45), p \equiv 1(\mathrm{mod}3), \\ p^2(2p^2-5p+3), \quad p \equiv 2(\mathrm{mod}3), \end{cases} \quad p \geq 5,$$

$$\sum_{s=1}^{p}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1} e(\frac{ma^8+sa^4+na}{p})\right|^4 = \begin{cases} p^2(2p^2-25p+96), \quad p \equiv 1(\mathrm{mod}4), \\ p^2(2p^2-11p+16), \quad p \equiv 3(\mathrm{mod}4), \end{cases} \quad p \geq 7.$$

3 定理 1.1 的另一种证明

这一部分将给出三项指数和的四次均值

$$\sum_{s=1}^{p}\sum_{m=1}^{p}\left|{\sum_{a=1}^{p}}' e(\frac{ma^k+sa^t+na}{p})\right|^4$$

在 $k=2t$ 时的简化证明方法.

当 $k=2t$ 时, 有

$$\sum_{s=1}^{p}\sum_{m=1}^{p}\left|\sum_{a=1}^{p}{}'e(\frac{ma^k+sa^t+na}{p})\right|^4=\sum_{s=1}^{p}\sum_{m=1}^{p}\left|\sum_{a=1}^{p}{}'e(\frac{ma^{2t}+sa^t+na}{p})\right|^4$$

$$=\sum_{m=1}^{p}\sum_{s=1}^{p}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1}e(\frac{m(a^{2t}+b^{2t}-c^{2t}-d^{2t})+s(a^t+b^t-c^t-d^t)+n(a+b-c-d)}{p})$$

$$=p^2\sum_{\substack{a^{2t}+b^{2t}\equiv c^{2t}+d^{2t}(\mathrm{mod}p)\\ a^t+b^t\equiv c^t+d^t(\mathrm{mod}p)}}^{p-1}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1}e(\frac{n(a+b-c-d)}{p})$$

$$=p^2\sum_{\substack{a^{2t}+b^{2t}\equiv c^{2t}+d^{2t}(\mathrm{mod}p)\\ a^t+b^t\equiv c^t+d^t(\mathrm{mod}p)}}^{p-1}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1}e(\frac{n(a+b-c-d)}{p})$$

$$=p^2\sum_{\substack{a^{2t}+b^{2t}\equiv c^{2t}+1\,(\mathrm{mod}p)\\ a^t+b^t\equiv c^t+1\,(\mathrm{mod}p)}}^{p-1}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1}e(\frac{nd(a+b-c-1)}{p})$$

$$=p^2\sum_{\substack{a^{2t}+b^{2t}\equiv c^{2t}+1\,(\mathrm{mod}p)\\ a^t+b^t\equiv c^t+1\,(\mathrm{mod}p)\\ a+b\equiv c+1\ (\mathrm{mod}\ p)}}^{p-1}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}e(\frac{nd(a+b-c-1)}{p})$$

$$-p^2\sum_{\substack{a^{2t}+b^{2t}\equiv c^{2t}+1\,(\mathrm{mod}p)\\ a^t+b^t\equiv c^t+1\,(\mathrm{mod}p)}}^{p-1}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}e(\frac{nd(a+b-c-1)}{p})$$

$$=p^2\sum_{\substack{(a^t-1)(b^t-1)\equiv 0(\mathrm{mod}p)\\ a^t+b^t\equiv c^t+1\,(\mathrm{mod}p)}}^{p-1}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}e(\frac{nd(a+b-c-1)}{p})$$

$$-p^2\sum_{\substack{(a^t-1)(b^t-1)\equiv 0(\mathrm{mod}p)\\ a^t+b^t\equiv c^t+1\,(\mathrm{mod}p)\\ a+b\equiv c+1\ (\mathrm{mod}\ p)}}^{p-1}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}e(\frac{nd(a+b-c-1)}{p}),$$

上式的计算可归结为求解同余方程组的问题, 经分析和计算亦可获得命题 1.1 及定理 1.1 中

的结果, 此处不再展开讨论.

本文进一步深入研究了三项指数和四次均值

$$\sum_{s=1}^{p}\sum_{m=1}^{p}\left|\sum_{a=1}^{p-1}e(\frac{ma^k+sa^t+na}{p})\right|^4$$

的计算问题, 获得了 $k=2t,(k,p-1)=3,4$ 时的精确计算公式, 推广了论文 [14] 中的结果. 下一步将用本文提出的方法研究

$$\sum_{s=1}^{p}\sum_{m=1}^{p}\left|\sum_{a=1}^{p^\alpha}{}'e(\frac{ma^{2t}+sa^t+na}{p^\alpha})\right|^4,\alpha\geq 2$$

的计算问题. 本文所使用的思想和方法对于四项指数和与更多项指数和也有一定的借鉴作用, 但其算法复杂度大大增加.

参 考 文 献

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

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

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

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

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

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

[7] 王婷婷, 张文鹏. 关于四次及六次混合指数和的均值 [J]. 中国科学: 数学, 2011, 41(3): 265–270.

[8] 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 The., 2007, 123(2): 352–362.

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

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

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

[12] Mordedd L J. Rational functions representing all residues modp[J]. Proc. Amer. Math. Soc., 1972, 35(2): 411–412.

[13] 陈华. 基于身份的公钥密码系统的研究 [D]. 武汉: 武汉大学, 2012.

[14] Ai X C, Chen J H, Chen H, Zhang S L. Explicit formulas for the fourth moment of three-term exponential sums[C]. 应用数学与统计研究国际会议, 2014.

[15] 艾小川, 陈建华, 张四兰, 陈华. 三项指数和与同余方程组的关系的研究 [J]. 数学杂志, 2013, 33(3): 535–540.

[16] 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.

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

RESEARCHING THE RELATION BETWEEN THE THREE-TERM EXPONENTIAL SUMS AND THE SYSTEM OF THE CONGRUENCE EQUATIONS

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

(*1.School of Science, Navy 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: In this paper, the computation problem of the fourth power mean of the three-term exponential sums is further studied. By using the properties of exponential sums and various techniques and methods of solving the system of congruence equations, two explicit formulas of mean value are given throughout two different methods. Moreover, the essential relation between the fourth moment and the system of congruence equations is discovered.

Keywords: three-term exponential sum; fourth power mean; transform formula; the system of congruence equations

2010 MR Subject Classification: 11T23; 11T24