关于四次及六次混合指数和的均值

王婷婷*, 张文鹏

西北大学数学系, 西安 710127

E-mail: tingtingwang126@126.com, wpzhang@nwu.edu.cn

收稿日期: 2010-09-28; 接受日期: 2011-01-15; * 通信作者

国家自然科学基金 (批准号: 11071194) 资助项目

摘要 本文的主要目的是运用初等及代数方法研究四次及六次混合指数和的均值计算问题, 并给出几个有趣的计算公式和转换公式.

关键词 混合指数和 四次均值 六次均值 计算公式 转换公式

MSC (2010) 主题分类 11L03, 11L07

1 引言

设 $q \geq 3$ 是一个正整数. 对任意整数 m, n 及正整数 k , 混合指数和 $C(m, n, k; q)$ 由

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

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

关于 $C(m, n, k; q)$ 的各种性质, 许多学者进行过研究 (参阅文献 [1–8]). 例如 Weil^[1] 的经典工作给出了: 对所有素数 $p \nmid m$, $|C(m, n, k; p)| \leq k \cdot \sqrt{p}$. Cochrane 和 Zheng^[5] 证明了 $|C(m, n, k; p^\alpha)| \leq k \cdot p^{\frac{2}{3}\alpha}(n, p^\alpha)^{\frac{1}{3}}$.

本文中将研究当整数 $k = 2$ 及 3 时, 均值 $\sum_{m=1}^p |C(m, n, k; p)|^{2r}$ 的计算问题, 并给出两个精确的计算公式和转换公式. 主要结果如下:

定理 1 设 p 是奇素数. 对任意整数 n , 若 $(n, p) = 1$, 则有恒等式

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

定理 2 设 p 是奇素数. 对任意整数 n , 若 $(n, p) = 1$ 且 $3 \nmid p-1$, 则有恒等式

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

定理 3 设 p 是奇素数. 对任意整数 n , 若 $(n, p) = 1$, 则有转换公式

(A) 若 $p \equiv 3 \pmod{4}$, 则有

$$\sum_{m=1}^p |C(m, n, 2; p)|^6 = p^4 - p^3 - p^2 - 8p \\ - p^2 \sum_{a=1}^{p-2} \sum_{c=1}^{p-2} \sum_{e=1}^{p-2} \left(\frac{ace((c+2)(e+2)a + (c+2)(a+2)e + (a+2)(e+2)c)}{p} \right);$$

(B) 若 $p \equiv 1 \pmod{4}$, 则有

$$\sum_{m=1}^p |C(m, n, 2; p)|^6 = p^4 - p^3 - 14p^2 - 20p \\ + p^2 \sum_{a=1}^{p-2} \sum_{c=1}^{p-2} \sum_{e=1}^{p-2} \left(\frac{ace((c+2)(e+2)a + (c+2)(a+2)e + (a+2)(e+2)c)}{p} \right),$$

其中 $\left(\frac{x}{p}\right)$ 表示 Legendre 符号.

对整数 $k \geq 4$ 及 $r \geq 3$, 利用本文的方法以及复杂的计算我们有可能给出均值

$$\sum_{m=1}^p |C(m, n, k; p)|^{2r}$$

的一个计算公式, 这将是进一步研究的目标.

本文中的定理及其证明过程虽然简单, 但是对研究此类问题, 特别是高次均值等内容研究提出了一个新的研究方法, 即定理 3 中的转换公式. 这一方法对研究其它混合指数和的高次均值的计算也有借鉴作用, 甚至用文献 [9, 10] 中的方法还可以给出高次均值的渐近公式.

2 定理的证明

本节将完成所有定理的证明. 首先证明定理 1. 显然, 对任意整数 r , 若 $(r, p) = 1$, 则有

$$\begin{aligned} \sum_{m=1}^p |C(m, n, 2; p)|^4 &= \sum_{m=1}^p \left| \sum_{a=1}^{p-1} e\left(\frac{m\bar{r}^2 a^2 + na}{p}\right) \right|^4 \\ &= \frac{1}{p-1} \sum_{m=1}^p \sum_{r=1}^{p-1} \left| \sum_{a=1}^{p-1} e\left(\frac{m\bar{r}^2 (ra)^2 + n(ra)}{p}\right) \right|^4 \\ &= \frac{1}{p-1} \sum_{m=1}^p \sum_{r=1}^{p-1} \left| \sum_{a=1}^{p-1} e\left(\frac{ma^2 + nra}{p}\right) \right|^4 \\ &= \frac{1}{p-1} \sum_{m=1}^p \sum_{r=1}^p \left| \sum_{a=1}^{p-1} e\left(\frac{ma^2 + nra}{p}\right) \right|^4 - \frac{1}{p-1} \sum_{m=1}^p \left| \sum_{a=1}^{p-1} e\left(\frac{ma^2}{p}\right) \right|^4 \\ &\equiv S_1 - S_2, \end{aligned} \quad (2.1)$$

其中 $\bar{r}$ 表示同余方程 $xr \equiv 1 \pmod{p}$ 的解. 当 $p \equiv 3 \pmod{4}$ 时, 设 χ_2 表示 Legendre 符号, 注意到 Gauss 和 $\tau(\chi_2) = i\sqrt{p}$, 我们可得

$$S_2 = \frac{1}{p-1} \sum_{m=1}^p \left| \sum_{a=1}^{p-1} e\left(\frac{ma^2}{p}\right) \right|^4$$

$$\begin{aligned}
&= (p-1)^3 + \frac{1}{p-1} \sum_{m=1}^{p-1} \left| \sum_{a=1}^{p-1} e\left(\frac{ma}{p}\right) + \sum_{a=1}^{p-1} \chi_2(a) e\left(\frac{ma}{p}\right) \right|^4 \\
&= (p-1)^3 + \frac{1}{p-1} \sum_{m=1}^{p-1} |-1 + \chi_2(m)\tau(\chi_2)|^4 \\
&= (p-1)^3 + (p+1)^2.
\end{aligned} \tag{2.2}$$

当 $p \equiv 1 \pmod{4}$ 时, 由 Gauss 和 $\tau(\chi_2) = \sqrt{p}$, 我们有

$$\begin{aligned}
S_2 &= \frac{1}{p-1} \sum_{m=1}^p \left| \sum_{a=1}^{p-1} e\left(\frac{ma^2}{p}\right) \right|^4 \\
&= (p-1)^3 + \frac{1}{p-1} \sum_{m=1}^{p-1} |-1 + \chi_2(m)\tau(\chi_2)|^4 \\
&= (p-1)^3 + (p^2 + 6p + 1).
\end{aligned} \tag{2.3}$$

现在我们计算 S_1 . 由三角和的性质可得

$$\begin{aligned}
S_1 &= \frac{1}{p-1} \sum_{m=1}^p \sum_{r=1}^p \left| \sum_{b=1}^{p-1} \sum_{a=1}^{p-1} e\left(\frac{ma^2 - mb^2 + nra - nrb}{p}\right) \right|^2 \\
&= \frac{1}{p-1} \sum_{m=1}^p \sum_{r=1}^p \left| (p-1) + \sum_{a=2}^{p-1} \sum_{b=1}^{p-1} e\left(\frac{mb^2(a^2-1) + rb(a-1)}{p}\right) \right|^2 \\
&= \frac{1}{p-1} \sum_{m=1}^p \sum_{r=1}^p \left| (p-1) + \sum_{a=2}^{p-1} \sum_{b=1}^{p-1} e\left(\frac{mb^2\overline{a-1}(a+1) + rb}{p}\right) \right|^2 \\
&= \frac{1}{p-1} \sum_{m=1}^p \sum_{r=1}^p \sum_{a=2}^{p-1} \sum_{b=1}^{p-1} \sum_{c=2}^{p-1} \sum_{d=1}^{p-1} e\left(\frac{m(b^2\overline{a-1}(a+1) - d^2\overline{c-1}(c+1)) + r(b-d)}{p}\right) \\
&\quad + (p-1)p^2 + \frac{p-1}{p-1} \sum_{m=1}^p \sum_{r=1}^p \sum_{a=2}^{p-1} \sum_{b=1}^{p-1} e\left(\frac{mb^2\overline{a-1}(a+1) + rb}{p}\right) \\
&\quad + \frac{p-1}{p-1} \sum_{m=1}^p \sum_{r=1}^p \sum_{c=2}^{p-1} \sum_{d=1}^{p-1} e\left(\frac{-md^2\overline{c-1}(c+1) - rd}{p}\right) \\
&= (p-1)p^2 + p^2 \sum_{\substack{a=2 \\ \overline{a-1}(a+1) \equiv \overline{c-1}(c+1) \pmod{p}}}^{p-1} \sum_{c=2}^{p-1} 1 \\
&= (p-1)p^2 + p^2(p-2).
\end{aligned} \tag{2.4}$$

结合 (2.1)–(2.4) 式, 我们立刻得到

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

于是证明了定理 1.

下面证明定理 2. 注意到对任意整数 k 且成立 $(k, p-1) = 1$ 时, 有

$$\frac{1}{p-1} \sum_{m=1}^p \left| \sum_{a=1}^{p-1} e\left(\frac{ma^k}{p}\right) \right|^4 = (p-1)^3 + \frac{1}{p-1} \sum_{m=1}^{p-1} \left| \sum_{a=1}^{p-1} e\left(\frac{ma}{p}\right) \right|^4 = (p-1)^3 + 1$$

及

$$\begin{aligned}
 & \frac{1}{p-1} \sum_{m=1}^p \sum_{r=1}^p \left| \sum_{b=1}^{p-1} \sum_{a=1}^{p-1} e\left(\frac{ma^3 - mb^3 + nra - nr b}{p}\right) \right|^2 \\
 &= \frac{1}{p-1} \sum_{m=1}^p \sum_{r=1}^p \left| (p-1) + \sum_{a=2}^{p-1} \sum_{b=1}^{p-1} e\left(\frac{mb^3(a^3-1) + rb(a-1)}{p}\right) \right|^2 \\
 &= (p-1)p^2 + p^2 \sum_{a=2}^{p-1} \sum_{c=2}^{p-1} 1 \\
 & \quad \overline{a-1}^3(a^3-1) \equiv \overline{c-1}^3(c^3-1) \pmod{p} \\
 &= (p-1)p^2 + p^2(2p-5).
 \end{aligned}$$

因此,

$$\begin{aligned}
 \sum_{m=1}^p |C(m, n, 3; p)|^4 &= \frac{1}{p-1} \sum_{m=1}^p \sum_{r=1}^{p-1} \left| \sum_{a=1}^{p-1} e\left(\frac{ma^3 + nra}{p}\right) \right|^4 \\
 &= \frac{1}{p-1} \sum_{m=1}^p \sum_{r=1}^p \left| \sum_{a=1}^{p-1} e\left(\frac{ma^3 + ra}{p}\right) \right|^4 - \frac{1}{p-1} \sum_{m=1}^p \left| \sum_{a=1}^{p-1} e\left(\frac{ma^3}{p}\right) \right|^4 \\
 &= (p-1)p^2 + p^2(2p-5) - (p-1)^3 - 1 \\
 &= 2p^3 - 3p^2 - 3p.
 \end{aligned}$$

即证明了定理 2.

现在我们证明定理 3. 与定理 1 的证明方法类似, 我们有

$$\begin{aligned}
 \sum_{m=1}^p |C(m, n, 2; p)|^6 &= \sum_{m=1}^p \left| \sum_{a=1}^{p-1} e\left(\frac{m\bar{r}^2 a^2 + na}{p}\right) \right|^6 \\
 &= \frac{1}{p-1} \sum_{m=1}^p \sum_{r=1}^{p-1} \left| \sum_{a=1}^{p-1} e\left(\frac{ma^2 + nra}{p}\right) \right|^6 \\
 &= \frac{1}{p-1} \sum_{m=1}^p \sum_{r=1}^p \left| \sum_{a=1}^{p-1} e\left(\frac{ma^2 + nra}{p}\right) \right|^6 - \frac{1}{p-1} \sum_{m=1}^p \left| \sum_{a=1}^{p-1} e\left(\frac{ma^2}{p}\right) \right|^6 \\
 &\equiv W_1 - W_2.
 \end{aligned} \tag{2.5}$$

现在分别计算 (2.5) 式中 W_1 和 W_2 . 若 $p \equiv 3 \pmod{4}$, 则有

$$W_2 = (p-1)^5 + (p+1)^3. \tag{2.6}$$

若 $p \equiv 1 \pmod{4}$, 则有

$$W_2 = (p-1)^5 + p^3 + 15p^2 + 15p + 1. \tag{2.7}$$

另一方面, 由三角和的性质还可得到

$$W_1 = \frac{1}{p-1} \sum_{m=1}^p \sum_{r=1}^p \left| \sum_{a=1}^{p-1} e\left(\frac{ma^2 + ra}{p}\right) \right|^6$$

$$\begin{aligned}
&= \frac{1}{p-1} \sum_{m=1}^p \sum_{r=1}^p \left((p-1) + \sum_{a=2}^{p-1} \sum_{b=1}^{p-1} e \left(\frac{mb^2(a^2-1) + rb(a-1)}{p} \right) \right)^3 \\
&= \frac{1}{p-1} \sum_{m=1}^p \sum_{r=1}^p \left((p-1) + \sum_{a=2}^{p-1} \sum_{b=1}^{p-1} e \left(\frac{mb^2 \overline{a-1}(a+1) + rb}{p} \right) \right)^3 \\
&= (p-1)^2 p^2 + 3 \sum_{m=1}^p \sum_{r=1}^p \left(\sum_{a=2}^{p-1} \sum_{b=1}^{p-1} e \left(\frac{mb^2 \overline{a-1}(a+1) + rb}{p} \right) \right)^2 \\
&\quad + \frac{1}{p-1} \sum_{m=1}^p \sum_{r=1}^p \left(\sum_{a=2}^{p-1} \sum_{b=1}^{p-1} e \left(\frac{mb^2 \overline{a-1}(a+1) + rb}{p} \right) \right)^3 \\
&\equiv (p-1)^2 p^2 + W_{11} + W_{12}.
\end{aligned} \tag{2.8}$$

由定理 2、(2.2) 式及定理 2 的证明方法可得

$$W_{11} = 3 \sum_{m=1}^p \sum_{r=1}^p \left(\sum_{a=2}^{p-1} \sum_{b=1}^{p-1} e \left(\frac{mb^2 \overline{a-1}(a+1) + rb}{p} \right) \right)^2 = 3p^2(p-1)(p-2). \tag{2.9}$$

注意到对任意整数 a, b 及 c , 且 $(a, p) = 1$, 同余方程 $ax^2 + bx + c \equiv 0 \pmod{p}$ 有 $1 + (\frac{b^2-4ac}{p})$ 个整数解, 这里 $(\frac{x}{p})$ 表示 Legendre 符号.

所以由 (2.1) 式及模 p 的完全剩余系的性质可得

$$\begin{aligned}
W_{12} &= \frac{1}{p-1} \sum_{m=1}^p \sum_{r=1}^p \left(\sum_{a=2}^{p-1} \sum_{b=1}^{p-1} e \left(\frac{mb^2 \overline{a-1}(a+1) + rb}{p} \right) \right)^3 \\
&= p^2 \sum_{a=2}^{p-1} \sum_{c=2}^{p-1} \sum_{e=2}^{p-1} \sum_{d=1}^{p-2} 1 \\
&\quad (a+1)(c-1)(e-1)+d^2(c+1)(a-1)(e-1)+(d+1)^2(e+1)(a-1)(c-1) \equiv 0 \pmod{p} \\
&= p^2 \sum_{a=1}^{p-2} \sum_{c=1}^{p-2} \sum_{e=1}^{p-2} \sum_{d=1}^{p-2} 1 \\
&\quad (a+2)ce+d^2(c+2)ae+(d+1)^2(e+2)ac \equiv 0 \pmod{p} \\
&= -2p^2(p-2)^2 + p^2 \sum_{a=1}^{p-2} \sum_{c=1}^{p-2} \sum_{e=1}^{p-2} \sum_{d=1}^p 1 \\
&\quad (a+2)ce+d^2(c+2)ae+(d+1)^2(e+2)ac \equiv 0 \pmod{p} \\
&= p^2 \sum_{a=1}^{p-2} \sum_{c=1}^{p-2} \sum_{e=1}^{p-2} \left(\frac{(e+2)^2 a^2 c^2 - ((c+2)ae + (e+2)ac)((a+2)ec + (e+2)ac)}{p} \right) \\
&\quad - 2p^2(p-2)^2 + p^2(p-2)^3 + p^2(p-2)(p-3) + p^3 \\
&= p^2 \sum_{a=1}^{p-2} \sum_{c=1}^{p-2} \sum_{e=1}^{p-2} \left(\frac{(e+2)^2 a^2 c^2 - ((c+2)ae + (e+2)ac)((a+2)ec + (e+2)ac)}{p} \right) \\
&\quad - 2p^2(p-2)^2 + p^2(p-2)^3 + p^3 \\
&= p^2 \sum_{a=1}^{p-2} \sum_{c=1}^{p-2} \sum_{e=1}^{p-2} \left(\frac{-ace((c+2)(e+2)a + (c+2)(a+2)e + (a+2)(e+2)c)}{p} \right) \\
&\quad - 2p^2(p-2)^2 + p^2(p-2)^3 + p^3.
\end{aligned} \tag{2.10}$$

当 $p \equiv 3 \pmod{4}$ 时有 $(\frac{-1}{p}) = -1$. 结合 (2.5)、(2.6)、(2.8)–(2.10) 式立刻推出恒等式

$$\sum_{m=1}^p |C(m, n, 2; p)|^6 = p^4 - p^3 - p^2 - 8p - p^2 \sum_{a=1}^{p-2} \sum_{c=1}^{p-2} \sum_{e=1}^{p-2} \left(\frac{ace((c+2)(e+2)a + (c+2)(a+2)e + (a+2)(e+2)c)}{p} \right). \quad (2.11)$$

当 $p \equiv 1 \pmod{4}$ 时有 $(\frac{-1}{p}) = 1$. 由 (2.5)、(2.7)–(2.10) 式我们有恒等式

$$\sum_{m=1}^p |C(m, n, 2; p)|^6 = p^4 - p^3 - 14p^2 - 20p + p^2 \sum_{a=1}^{p-2} \sum_{c=1}^{p-2} \sum_{e=1}^{p-2} \left(\frac{ace((c+2)(e+2)a + (c+2)(a+2)e + (a+2)(e+2)c)}{p} \right). \quad (2.12)$$

现在由恒等式 (2.11) 及 (2.12) 式不难推出定理 3. 于是完成了定理的证明.

致谢 作者对审稿人提出的宝贵意见和建议表示衷心的感谢.

参考文献

- 1 Weil A. On some exponential sums. Proc Nat Acad Sci USA, 1948, 34: 204–207
- 2 Cochrane T, Zheng Z. Bounds for certain exponential sums. Asian J Math, 2000, 4: 757–773
- 3 Cochrane T, Zheng Z. Pure and mixed exponential sums. Acta Arith, 1999, 91: 249–278
- 4 Cochrane T, Zheng Z. Exponential sums with rational function entries. Acta Arith, 2000, 95: 67–95
- 5 Cochrane T, Zheng Z. Upper bounds on a two-term exponential sums. Sci China Ser A, 2001: 44: 1003–1015
- 6 Cochrane T. Exponential sums modulo prime powers. Acta Arith, 2002, 101: 131–149
- 7 Cochrane T, Pinner C. A further refinement of Mordell's bound on exponential sums. Acta Arith, 2005, 116: 35–41
- 8 Cochrane T, Pinner C. Using Stepanov's method for exponential sums involving rational functions. J Number Theory, 2006, 116: 270–292
- 9 Katz N M. Estimates for nonsingular multiplicative character sums. Internat Math Res Not, 2002, 7: 333–349
- 10 Schmidt W M. Equations over Finite Fields: An Elementary Approach. Lecture Notes in Mathematics, vol. 536. Berlin: Springer-Verlag, 1976

On the fourth and sixth power mean of mixed exponential sums

WANG TingTing & ZHANG WenPeng

Abstract In this paper, the computational problems of the mixed exponential sums is studied. Two exact computation formulae and conversion formulae for the fourth and sixth power mean of the mixed exponential sums are given.

Keywords: mixed exponential sums, fourth power mean, sixth power mean, computational formula, conversion formula

MSC(2000): 11L03, 11L07

doi: 10.1360/012010-753