Chin. Ann. Math.
25B:1(2004),97–102.

ON THE GENERAL k-TH KLOOSTERMAN SUMS AND ITS FOURTH POWER MEAN***

LIU Hongyan* ZHANG Wenpeng**

Abstract

The main purpose of this paper is to study the asymptotic property of the fourth power mean of the general k-th Kloosterman sums, and give an interesting asymptotic formula.

Keywords General k-th Kloosterman sums, Fourth power mean, Asymptotic formula
2000 MR Subject Classification 11F20
Chinese Library Classification O156.4
Document Code A
Article ID 0252-9599(2004)01-0097-06

§ 1 . Introduction

Let $q \geq 3$ be a positive integer. For any integers m, n and k , we define the general k-th Kloosterman sums $S(m,n,k,\chi;q)$ as follows:

$$S(m,n,k,\chi;q) = {\sum_{a=1}^{q}}' \chi(a) e\Big(\frac{ma^k + n\overline{a}^k}{q}\Big),$$

where $\sum'$ denotes the summation over all a such that $(a,q)=1$, $a\overline{a} \equiv 1 \bmod q$, χ denotes a Dirichlet character mod q and $e(y) = e^{2\pi i y}$.

This summation is very important, because it is a generalization of the classical Kloosterman sums $S(m,n,1,\chi_0;q) = S(m,n;q)$, where χ_0 is the principal character mod q. The various properties of $S(m,n;q)$ were investigated by many authors. Perhaps the most famous property of $S(m,n;q)$ is the estimate (see [1, 2]):

$$|S(m,n;q)| \leq d(q) q^{\frac{1}{2}} (m,n,q)^{\frac{1}{2}}, \tag{1.1}$$

where $d(q)$ is the divisor function, (m,n,q) denotes the greatest common divisor of m, n and q. If q is a prime p, then S. Chowla [3] and A. V. Malyshev [4] also proved a similar result for $S(m,n,1,\chi;p)$. But about the properties of $S(m,n,k,\chi;q)$ for general mod q, we know

Manuscript received November 1, 2002.
*Department of Mathematics, Northwest University, Xi'an 710069, China. **E-mail:** lhysms@sina.com
Department of Applied Mathematics, Xi'an University of Technology, Xi'an 710048, China.
**Department of Mathematics, Northwest University, Xi'an 710069, China.
E-mail: wpzhang@nwu.edu.cn
***Project supported by the National Natural Science Foundation of China (No.10271093) and the Shanxi Provincial Natural Science Foundation of China.

very little at present, even if we do not know how large $|S(m,n,k,\chi;q)|$ is. On the other hand, H. Iwaniec [5] studied the fourth power mean of $S(m,n;q)$, and proved the identity

$$\sum_{a=1}^{p-1} S^4(a,1;p) = 2p^3 - 3p^2 - 3p - 1.$$

H. Salié [6] and H. Davenport (independently) obtained the estimate

$$\sum_{a=1}^{p-1} S^6(a,1;p) \ll p^4.$$

The main purpose of this paper is to study the asymptotic properties of the $2l$-th power mean

$$\sum_{\chi \bmod q} \sum_{m=1}^{q} |\ S(m,n,k,\chi;q)\ |^{2l}, \tag{1.2}$$

and gives an exact formula for (1.2) with $l = 2$. That is, we shall prove the following

Theorem. *Let $q \geq 3$ be an integer. Then for any fixed integer n and k with $(nk,q) = 1$, we have the identity*

$$\sum_{\chi \bmod q} \sum_{m=1}^{q} |\ S(m,n,k,\chi;q)\ |^{4}$$
$$= \phi^2(q) q^2 \prod_{p^\alpha \| q} (k, p-1)^2 \Big(\alpha - 1 + \frac{2(p-1)}{(k,p-1)p} + \frac{\alpha}{p^\alpha} - \frac{2(p^\alpha - 1)}{p^\alpha (p-1)} \Big),$$

where $\phi(q)$ is the Euler function, $\prod_{p^\alpha \| q}$ denotes the product over all p such that $p^\alpha \mid q$ and $p^{\alpha+1} \nmid q$.

For general integer $l \geq 3$ and $(nk,q) = 1$, whether there exists an exact formula for (1.2) is an open problem.

§ 2 . Some Lemmas

To complete the proof of the theorem, we need the following Lemmas.

Lemma 2.1. *Let p be a prime, α and k be any positive integer with $(k,p) = 1$. Then we have the identity*

$$\mathop{{\sum}'}_{\substack{a=1 \\ p^\alpha | (a^k-1)(b^k-1)}}^{p^\alpha} \mathop{{\sum}'}_{b=1}^{p^\alpha} 1 = d^2 p^\alpha \Big(\alpha - 1 + \frac{2(p-1)}{dp} + \frac{\alpha}{p^\alpha} - \frac{2(p^\alpha - 1)}{p^\alpha (p-1)} \Big),$$

where $d = (k, \phi(p^\alpha))$.

Proof. If $\alpha = 1$, then we have

$$\mathop{{\sum}'}_{\substack{a=1 \\ p | (a^k-1)(b^k-1)}}^{p} \mathop{{\sum}'}_{b=1}^{p} 1 = \sum_{\substack{a=1 \\ p | (a^k-1)(b^k-1)}}^{p-1} \sum_{b=1}^{p-1} 1 = 2d(p-1) - d^2.$$

So Lemma 2.1 holds for $\alpha = 1$. Now we suppose $\alpha \geq 2$. From the properties of the Möbius function (see [7]), we immediately get

$$\begin{aligned}
\sideset{}{'}\sum_{\substack{a=1 \\ p^\alpha|(a^k-1)(b^k-1)}}^{p^\alpha} \sideset{}{'}\sum_{b=1}^{p^\alpha} 1 &= \sum_{\substack{a=1 \\ p^\alpha|(a^k-1)(b^k-1)}}^{p^\alpha} \sum_{b=1}^{p^\alpha} \sum_{t|(a,p^\alpha)} \mu(t) \sum_{h|(b,p^\alpha)} \mu(h) \\
&= \sum_{t|p^\alpha} \mu(t) \sum_{h|p^\alpha} \mu(h) \sum_{\substack{a=1 \\ p^\alpha|((ta)^k-1)((hb)^k-1)}}^{p^\alpha/t} \sum_{b=1}^{p^\alpha/h} 1 \\
&= \sum_{\substack{a=1 \\ p^\alpha|(a^k-1)(b^k-1)}}^{p^\alpha} \sum_{b=1}^{p^\alpha} 1 - 2d \sum_{a=1}^{p^{\alpha-1}} 1 \\
&= 2dp^\alpha - d^2 + \sum_{i=1}^{\alpha-1} \sum_{\substack{a=1 \\ p^i|(a^k-1) \\ a^k \neq 1}}^{p^\alpha} \sum_{\substack{b=1 \\ p^{\alpha-i}|(b^k-1) \\ b^k\neq 1}}^{p^\alpha} 1 - 2dp^{\alpha-1}. \qquad (2.1)
\end{aligned}$$

Noting that $(a, p^\alpha) = 1$, we have $a = g^l$, where g is a primitive root of p^α. So we have

$$\begin{aligned}
\sum_{\substack{a=1 \\ p^i|(a^k-1) \\ a^k\neq 1}}^{p^\alpha} &= \sum_{\substack{a=1 \\ p^i|(a^k-1)}}^{p^\alpha} 1 - d = \sum_{\substack{l=0 \\ p^i|(g^{lk}-1)}}^{\phi(p^\alpha)-1} 1 - d = \sum_{\substack{l=0 \\ \phi(p^i)|lk}}^{\phi(p^\alpha)-1} 1 - d \\
&= \sum_{\substack{l=0 \\ \frac{\phi(p^i)}{d}|l}}^{\phi(p^\alpha)-1} 1 - d = d\frac{\phi(p^\alpha)}{\phi(p^i)} - d = d(p^{\alpha-i} - 1). \qquad (2.2)
\end{aligned}$$

Combining (2.1) and (2.2), we may get

$$\begin{aligned}
\sideset{}{'}\sum_{\substack{a=1 \\ p^\alpha|(a^k-1)(b^k-1)}}^{p^\alpha} \sideset{}{'}\sum_{b=1}^{p^\alpha} 1 &= 2dp^\alpha - d^2 + \sum_{i=1}^{\alpha-1} d^2(p^{\alpha-i}-1)(p^i-1) - 2dp^{\alpha-1} \\
&= d^2p^\alpha\Big(\alpha - 1 + \frac{2(p-1)}{dp} + \frac{\alpha}{p^\alpha} - \frac{2(p^\alpha-1)}{p^\alpha(p-1)}\Big).
\end{aligned}$$

This completes the proof of Lemma 2.1.

Lemma 2.2. *Let n, k, k_1, k_2 be integers with $(n, k_1k_2) = (k_1, k_2) = 1$. Then for any character χ mod k_1k_2, there exist integers n_1 and n_2 with $(n_1, k_1) = (n_2, k_2) = 1$ such that*

$$n \equiv n_1k_2^2 + n_2k_1^2 \pmod{k_1k_2},$$

and for these integers we have

$$| S(m, n, k, \chi; k_1k_2) | = | S(m\overline{k_2}, n_1k_2, k, \chi_1; k_1) | \cdot | S(m\overline{k_1}, n_2k_1, k, \chi_2; k_2) |,$$

where $\chi = \chi_1\chi_2$ with χ_1 mod k_1 and χ_2 mod k_2.

Proof. Since $(k_1, k_2) = 1$, we have $(k_1^2, k_2^2) = 1$. Therefore there exists integer n_1 such that $n_1 k_2^2 \equiv n \bmod k_1^2$, and n_2 such that $n_2 k_1^2 \equiv n \bmod k_2^2$. These imply that $k_1^2 \mid n_1 k_2^2 + n_2 k_1^2 - n$ and $k_2^2 \mid n_1 k_2^2 + n_2 k_1^2 - n$. That is,

$$n \equiv n_1 k_2^2 + n_2 k_1^2 \pmod{k_1 k_2}.$$

It is clear that $(k_1, n_1) = (k_1, n_1 k_2^2) = (k_1, n) = 1$ and $(k_2, n_2) = 1$.

Let $\chi = \chi_1 \chi_2$ with $\chi_1 \bmod k_1$ and $\chi_2 \bmod k_2$. Then for integers k_1, k_2, n_1 and n_2, we have

$$\begin{aligned}
&S(m, n, k, \chi; k_1 k_2)\\
&= \sum_{a=1}^{k_1}{}' \sum_{b=1}^{k_2}{}' \chi_1 \chi_2 (a k_2 + b k_1)\\
&\quad \cdot e\Big(\frac{m(ak_2 + bk_1)^k + (n_1 k_2^2 + n_2 k_1^2)\overline{(ak_2 + bk_1)^k}}{k_1 k_2}\Big)\\
&= \chi_1(k_2)\chi_2(k_1) \sum_{a=1}^{k_1}{}' \chi_1(a) e\Big(\frac{m a^k k_2^{k-1} + n_1 \overline{a^k}\,\overline{k_2^{k-1}}}{k_1}\Big)\\
&\quad \cdot \sum_{b=1}^{k_2}{}' \chi_1(b) e\Big(\frac{m b^k k_1^{k-1} + n_2 \overline{b^k}\,\overline{k_1^{k-1}}}{k_2}\Big)\\
&= \chi_1(k_2)\chi_2(k_1) \sum_{a=1}^{k_1}{}' \chi_1(a) e\Big(\frac{m a^k \overline{k_2} + n_1 \overline{a^k} k_2}{k_1}\Big)\\
&\quad \cdot \sum_{b=1}^{k_2}{}' \chi_1(b) e\Big(\frac{m b^k \overline{k_1} + n_2 \overline{b^k} k_1}{k_2}\Big)\\
&= \chi_1(k_2)\chi_2(k_1) S(m\overline{k_2}, n_1 k_2, k, \chi_1; k_1) S(m\overline{k_1}, n_2 k_1, k, \chi_2; k_2).
\end{aligned}$$

Then Lemma 2.2 follows from $\mid \chi_1(k_2)\chi_2(k_1) \mid = 1$.

Lemma 2.3. *Let p be a prime, and α a positive integer. Then for any integers k, n and v with $(knv, p) = 1$, we have*

$$\begin{aligned}
&\sum_{\chi \bmod p^\alpha} \sum_{m=1}^{p^\alpha} \mid S(m, nv, k, \chi; p^\alpha) \mid^4\\
&= \phi^2(p^\alpha) p^{2\alpha} d^2 \Big(\alpha - 1 + \frac{2(p-1)}{dp} + \frac{\alpha}{p^\alpha} - \frac{2(p^\alpha - 1)}{p^\alpha (p-1)}\Big),
\end{aligned}$$

where $d = (k, \phi(p^\alpha))$.

Proof. From the properties of characters, we have

$$\begin{aligned}
\mid S(m, n, k, \chi; q) \mid^2 &= \sum_{a=1}^{q}{}' \sum_{b=1}^{q}{}' \chi(a\overline{b}) e\Big(\frac{m(a^k - b^k) + n(\overline{a^k} - \overline{b^k})}{q}\Big)\\
&= \sum_{a=1}^{q}{}' \chi(a) \sum_{b=1}^{q}{}' e\Big(\frac{m b^k (a^k - 1) + n\overline{b^k}(\overline{a^k} - 1)}{q}\Big).
\end{aligned}$$

Now by the orthogonality relation for characters, we immediately get

$$\sum_{\chi \bmod q} | S(m,n,k,\chi;q) |^4$$
$$= \phi(q){\sum_{a=1}^{q}}' \Big| {\sum_{b=1}^{q}}' e\Big(\frac{mb^k(a^k-1)+n\overline{b^k}(\overline{a^k}-1)}{q}\Big)\Big|^2. \tag{2.3}$$

Note that the trigonometric identity

$$\sum_{a=1}^{q} e\Big(\frac{sa}{q}\Big) = \begin{cases} q, & \text{if } q \mid s; \\ 0, & \text{if } q \nmid s. \end{cases}$$

From (2.3) and Lemma 2.1, we have

$$\sum_{\chi \bmod p^\alpha} \sum_{m=1}^{p^\alpha} | S(m,nv,k,\chi;p^\alpha) |^4$$
$$= \phi(p^\alpha){\sum_{a=1}^{p^\alpha}}' \sum_{m=1}^{p^\alpha} \Big| {\sum_{b=1}^{p^\alpha}}' e\Big(\frac{mb^k(a^k-1)+nv\overline{b^k}(\overline{a^k}-1)}{p^\alpha}\Big)\Big|^2$$
$$= \phi(p^\alpha){\sum_{a=1}^{p^\alpha}}' {\sum_{b_1=1}^{p^\alpha}}' {\sum_{b_2=1}^{p^\alpha}}' \sum_{m=1}^{p^\alpha} e\Big(\frac{m(b_1^k-b_2^k)(a^k-1)+nv(\overline{b_1^k}-\overline{b_2^k})(\overline{a^k}-1)}{p^\alpha}\Big)$$
$$= \phi(p^\alpha){\sum_{a=1}^{p^\alpha}}' {\sum_{b_1=1}^{p^\alpha}}' {\sum_{b_2=1}^{p^\alpha}}' \sum_{m=1}^{p^\alpha} e\Big(\frac{mb_2^k(b_1^k-1)(a^k-1)+nv\overline{b_2^k}(\overline{b_1^k}-1)(\overline{a^k}-1)}{p^\alpha}\Big)$$
$$= \phi(p^\alpha){\sum_{a=1}^{p^\alpha}}' {\sum_{b_1=1}^{p^\alpha}}' {\sum_{b_2=1}^{p^\alpha}}' \sum_{m=1}^{p^\alpha} e\Big(\frac{mb_2^k(b_1^k-1)(a^k-1)+nv\overline{b_2^kb_1^ka^k}(1-b_1^k)(1-a^k)}{p^\alpha}\Big)$$
$$= \phi^2(p^\alpha)p^\alpha \mathop{{\sum_{a=1}^{p^\alpha}}' {\sum_{b=1}^{p^\alpha}}'}_{p^\alpha \mid (a^k-1)(b^k-1)} 1$$
$$= \phi^2(p^\alpha)p^{2\alpha}d^2\Big(\alpha - 1 + \frac{2(p-1)}{dp} + \frac{\alpha}{p^\alpha} - \frac{2(p^\alpha-1)}{p^\alpha(p-1)}\Big).$$

This proves Lemma 2.3.

§ 3. Proof of the Theorem

From Lemma 2.2 and Lemma 2.3 in the above section, we can complete the proof of the theorem. In fact, for any integers n and k with $(nk,q)=1$, let q have the prime power decomposition $q = \prod_{i=1}^{r} p_i^{\alpha_i}$, $m = \sum_{i=1}^{r} \frac{m_i q}{p_i^{\alpha_i}}$. It is clear that if m_i $(i=1,2,\cdots,r)$ pass through a complete residue system modulo $p_i^{\alpha_i}$, then m pass through a complete residue system modulo q. Note that $S(m,n_i,k,\chi_i;p_i^{\alpha_i}) = S(m_iq/p_i^{\alpha_i},n_i,k,\chi_i;p_i^{\alpha_i})$ and $(q/p_i^{\alpha_i},p_i^{\alpha_i}) = 1$.

From Lemma 2.2 and Lemma 2.3, we immediately obtain the identity

$$\begin{aligned}
&\sum_{\chi \bmod q} \sum_{m=1}^{q} \mid S(m,n,k,\chi;q) \mid^4 \\
&= \prod_{i=1}^{r} \Big[\sum_{\chi_i \bmod p_i^{\alpha_i}} \sum_{m_i=1}^{p_i^{\alpha_i}} \Big| S\Big(m_i \frac{q}{p_i^{\alpha_i}} \overline{\Big(\frac{q}{p_i^{\alpha_i}}\Big)}, n_i \frac{q}{p_i^{\alpha_i}}, k, \chi_i; p_i^{\alpha_i}\Big) \Big|^4 \Big] \\
&= \prod_{i=1}^{r} \Big[\sum_{\chi_i \bmod p_i^{\alpha_i}} \sum_{m_i=1}^{p_i^{\alpha_i}} \mid S(m_i, n_i q/p_i^{\alpha_i}, k, \chi_i; p_i^{\alpha_i}) \mid^4 \Big] \\
&= \prod_{i=1}^{r} \Big[\phi^2(p_i^{\alpha_i}) p_i^{2\alpha_i} d_i^2 \Big(\alpha_i - 1 + \frac{2(p_i-1)}{d_i p_i} + \frac{\alpha_i}{p_i^{\alpha_i}} - \frac{2(p_i^{\alpha_i}-1)}{p_i^{\alpha_i}(p_i-1)} \Big) \Big] \\
&= \phi^2(q) q^2 \prod_{p^\alpha \| q} (k, p-1)^2 \Big(\alpha - 1 + \frac{2(p-1)}{(k,p-1)p} + \frac{\alpha}{p^\alpha} - \frac{2(p^\alpha - 1)}{p^\alpha (p-1)} \Big).
\end{aligned}$$

This completes the proof of the theorem.

References

[1] Estermann, T., On Kloostermann's sum, *Mathematica*, **8**(1961), 83–86.

[2] Chalk, J. H. H. & Smith, R. A., On Bombieri's estimate for exponential sums, *Acta Arith.*, **18**(1971), 191–212.

[3] Chowla, S., On Kloosterman's sum, *Norkse Vid. Selbsk. Fak. Frondheim*, **40**(1967), 70–72.

[4] Malyshev, A. V., A generalization of Kloosterman sums and their estimates (in Russian), *Vestnik Leningrad Univ.*, **15**(1960), 59–75.

[5] Iwaniec, H., Topics in classical automorphic forms, *Graduate Studies in mathematics*, **17**(1997), 61–63.

[6] Salié, H., Uber die Kloostermanschen summen $S(u, v; q)$, *Math. Z.*, **34**(1931), 91–109.

[7] Apstol, T. M., Introduction to Analytic Number Theory, Springer-Verlag, New York, 1976.