Explicit formulas for the fourth power mean of certain two-term exponential sums

Xiaochuan Ai[1,2], Jianhua Chen[2*], Hua Chen[3], Silan Zhang[1,4]

[1]*School of Mathematics and Statistics, Wuhan University, Wuhan, 430072, Hubei, China*

[2]*School of Science, Navy University of Engineering, Wuhan, 430033, Hubei, China*

[3]*School of Science, Hubei University of Technology, Wuhan, 430068, Hubei, China*

[4]*College of Science, Huazhong Agricultural University, Wuhan 430070, Hubei, China*

Received 1 June 2014, www.cmnt.lv

Abstract

The aim of this paper is to obtain the explicit equations for the fourth power mean of generalized Kloosterman sums $\sum_{m=1}^{q}\sum_{\chi \bmod q}\sum_{\chi' \bmod q}\left|\sum_{a=1}^{q}{}'\chi(a)G(a,\chi')e\left(\frac{ma^k+na}{q}\right)\right|^4$, where $e(x)=e^{2\pi ix}$, χ and χ' are Dirichlet characters modulo q and $\sum_{a=1}^{q}{}'$ denotes the summation over all a with $(a,q)=1$, $G(a,\chi')$ is a Gauss sum. Moreover, this paper also acquires the computational formulas for the fourth power mean of two-term exponential sums $\sum_{m=1}^{q}\sum_{\chi \bmod q}|\sum_{a=1}^{q}{}'\chi(a)e\left(\frac{ma^k+na}{q}\right)|^4$. This improves Calderon and Xu's results by avoiding the restriction $(k,q)=1$.

Keywords: two-term exponential sums, Kloosterman sums, Dirichlet character, fourth power mean, gauss sum

1 Introduction

For integers m,n,q,k with $q\geq 3, k\geq 2$ and Dirichlet characters $\chi,\chi' \bmod q$, Calderon defined the generalized Kloosterman sums [1]

$$S(m,n,\chi,\chi',q)=\sum_{a=1}^{q}{}'\chi(a)G(a,\chi')e\left(\frac{ma^k+na}{q}\right), \qquad (1)$$

where $e(x)=e^{2\pi ix}$ and $\sum_{a=1}^{q}{}'$ denotes the summation over all a with $(a,q)=1$. Z. F. Xu defined a two-term exponential sums with Dirichlet character [2]:

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

The two-term exponential sums originally arose in connection with Waring's problem and the aim is to find optimal bounds. For example, as a pioneer work, Weil [3] proved:

$$|C(m,n,k,\chi;q)|\leq kq^{1/2},$$

where $q=p$ and $(m,p)=1$. If $q=p^\alpha$, $\alpha\geq 1$, $(m,p)=1$ and $k\geq 2$, it follows from T. Cochrane and Z. Zheng's work [4] that:

$$|C(m,n,k,\chi;p^\alpha)|\leq kp^{2/3\alpha}(n,p^\alpha)^{1/3}.$$

Besides, for $p=2$, they proved:

$$|C(m,n,k,\chi;2^\alpha)|\leq 2k2^{2/3\alpha}(n,2^\alpha)^{1/3},$$

and claimed that the exponent $\frac{2}{3}\alpha$ is the best result.

Though the single value of two-term exponential sums is irregular, the high power means of their values owns graceful arithmetical properties and it in turn become an interesting focus for many attentions. Calderon [1], Xu [2], Liu [5], Wang [6] acquired a lot of research results.

From Calderon and Xu's work, we have the following two Propositions:

Assumption 1: Let p be a prime with $(k,p)=(n,p)=1$ and $d=(k,p-1)$, let $S(m,n,\chi,\chi',p^\alpha)$ be the sums defined in (1). Then for any positive integer k, we have:

*** Corresponding author's** e-mail: lsyaiaxc@sohu.com

$$M_k(p^\alpha)=\sum_{m=1}^{p^\alpha}\sum_{\chi \bmod p^\alpha}\sum_{\chi' \bmod p^\alpha}\left|S(m,n,\chi,\chi',p^\alpha)\right|^4=$$
$$\begin{cases} p(p-1)^2[2p(p-d)-3p+d(d+2)][p(p-1)-1], \alpha=1 \\ p^{7\alpha-5}(p-1)^4[(\alpha+1)(p-1)-(2d-1)], \alpha\ge 2\end{cases}$$

Assumption 2: Let p be a prime with $(k,p)=(n,p)=1$ and $d=(k,p-1)$, let α be a positive integer. Then for any positive integer k, we have:

$$\sum_{m=1}^{p^\alpha}\sum_{\chi \bmod p^\alpha}|C(m,n,k,\chi;p^\alpha)|^4=$$
$$\begin{cases} p(p-1)^3[2-\frac{2d-1}{p-1}+\frac{d^2-1}{(p-1)^2}], \alpha=1 \\ p^\alpha\varphi^3(p^\alpha)(\alpha+1-\frac{2d-1}{p-1}), \alpha\ge 2\end{cases}.$$

Unfortunately, Calderon and Xu only got the explicit equations of $\sum_{m=1}^{p^\alpha}\sum_{\chi \bmod p^\alpha}\left|C(m,n,\chi,k,p^\alpha)\right|^4$ and $M_k(p^\alpha)$ under the condition of $(k,p)=1$, they haven't taken the situation $(k,p)=p$ into consideration. And for this reason, they can't give the explicit computational equations of $\sum_{m=1}^{q}\sum_{\chi \bmod q}\left|C(m,n,\chi,k,q)\right|^4$ and $M_k(q)$ if $(k,q)\ne 1$. The main purpose of this paper is to make further researches into the computation problem of the fourth power mean $M_k(p^\alpha)$ with the condition $(k,p)=p$ and thus obtain the computational equations of $M_k(q)$. Moreover, we acquire explicit equations of $\sum_{m=1}^{q}\sum_{\chi \bmod q}\left|C(m,n,\chi,k,q)\right|^4$ on the basis of $M_k(q)$. Now we list the main results.

Theorem 1 Let p be an odd prime with $(n,p)=1$, $(p,k)=p$ and $d=(k,p-1)$, let α be a positive integer. Then for any positive integer k, we have:

$$M_k(p^\alpha)=\sum_{m=1}^{p^\alpha}\sum_{\chi \bmod p^\alpha}\sum_{\chi' \bmod p^\alpha}\left|S(m,n,\chi,\chi',p^\alpha)\right|^4=$$
$$\begin{cases} p(p-1)^2(p^2-p-1)[2p(p-d)-3p+d(d+2)], \alpha=1 \\ p^{7\alpha-4}(p-1)^4, \alpha\ge 2\end{cases}$$

$$\sum_{m=1}^{p^\alpha}\sum_{\chi (\bmod p^\alpha)}\left|C(m,n,\chi,k,p^\alpha)\right|^4=$$
$$\begin{cases} p(p-1)^3\left[2-\frac{2d-1}{p-1}+\frac{d^2-1}{(p-1)^2}\right], \alpha=1 \\ p^{4\alpha-2}(p-1)^2, \alpha\ge 2\end{cases}.$$

2 Preliminaries

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

Lemma 1 Let p be a prime and α be any positive integer. Consider the Ramanujan sum

$$C_{p^\alpha}(n)=\sum_{v=1}^{p^\alpha}{}' e\left(\frac{nv}{p^\alpha}\right),$$

Then:

1) For $\alpha=1, C_p(n)=\sum_{v=1}^{p}{}' e(\frac{nv}{p})=\begin{cases}\varphi(p), p\mid n \\ -1, p\nmid n\end{cases}$.

2) For $\alpha\ge 2, C_{p^\alpha}(n)=\sum_{v=1}^{p^\alpha}{}' e\left(\frac{nv}{p^\alpha}\right)=\begin{cases}\varphi(p^\alpha), p^\alpha\mid n \\ -p^{\alpha-1}, p^{\alpha-1}\parallel n \\ 0, p^{\alpha-1}\nmid n\end{cases}$.

Proof: See the Theorem 7.4.4 in the Ref. [7].

Lemma 2 Let integer $q=p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_t^{\alpha_t}$, where $p_1,p_2,\cdots,p_t$ are positive integers, relatively prime in pairs: $(p_i,p_j)=1,\quad i\ne j,$ then we have:

$$\sum_{m=1}^{q}\sum_{\chi(\bmod q)}\left|C(m,n,\chi,k,q)\right|^4=$$
$$\prod_{i=1}^{t}\left(\sum_{\chi_i(\bmod p_i^{\alpha_i})}\sum_{m_i=1}^{p_i^{\alpha_i}}\left|\sum_{a=1}^{p_i^{\alpha_i}}{}'\chi_i(a)e\left(\frac{m_ia^k+na}{p_i^{\alpha_i}}\right)\right|^4\right),$$

where $\chi=\chi_1\chi_2\cdots\chi_t \bmod q$ such that $\chi_i \bmod p_i^{\alpha_i}$ $(i=1,2,\cdots,t)$.

Proof: See the Theorem 2.1 in the Ref. [2].

Lemma 3 Let p be a prime and k,α be positive integers, $S(m,n,\chi,\chi',p^\alpha)$ be the sum defined in (1), then we have the identity

$$M_k(p^\alpha)=\sum_{m=1}^{p^\alpha}\sum_{\chi \bmod p^\alpha}\sum_{\chi' \bmod p^\alpha}\left|S(m,n,\chi,\chi',p^\alpha)\right|^4= \quad (2)$$
$$p^{3\alpha-2}(p-1)^2N(p^\alpha)U(k;p^\alpha),$$

where:

$$N(p^\alpha)=\begin{cases}p^2-p-1, \alpha=1, \\ p^{2\alpha-1}(p-1), \alpha\ge 2\end{cases}$$

and

$$U(k;p^\alpha)=\sum_{\substack{c=1\\(c^k-1)(b^k-s^k)\equiv 0(\bmod p^\alpha)}}^{p^\alpha}{}'\sum_{b=1}^{p^\alpha}{}'\sum_{s=1}^{p^\alpha}{}' e\left(\frac{n(c-1)(b-s)}{p^\alpha}\right).$$

More, if $k=1$, then:

$$U(1;p^\alpha)=(\alpha+1)\varphi^2(p^\alpha)-\varphi(p^\alpha)p^{\alpha-1}.$$

Proof: See the Theorem 3.1 and Lemma 2.4 in [1].

Lemma 4 Let p be an odd prime and α, k be positive integers with $p^h \| k(h \ge 0)$. Let N denote the number of solutions of the system of congruencies:

$$\begin{cases} a^k \equiv 1(\bmod p^\alpha) \\ a \not\equiv 1(\bmod p) \end{cases}, \quad (3)$$

where a runs through a reduced residue system modulo p^α, then we have:

$$N = \begin{cases} (k, \varphi(p^\alpha)) - p^{\alpha-1}, & \alpha - 1 \le h, \\ (k, \varphi(p^\alpha)) - p^h, & \alpha - 1 > h. \end{cases}$$

Proof: Let g be a primitive root of modulo p and modulo p^α, let $a = g^i, 1 \le i \le \varphi(p^\alpha)$. Therefore, the system of congruencies Equation (3) equivalents to the system of congruencies:

$$\begin{cases} g^{ik} \equiv 1(\bmod p^\alpha) \\ g^i \not\equiv 1(\bmod p) \end{cases},$$

thus, we have:

$$\begin{cases} ik \equiv 0(\bmod \varphi(p^\alpha)) \\ i \not\equiv 0(\bmod \varphi(p)) \end{cases}.$$

Now we consider the number of the solutions of the system of congruencies

$$\begin{cases} ik \equiv 0(\bmod \varphi(p^\alpha)) \\ i \equiv 0(\bmod \varphi(p)) \end{cases}. \quad (4)$$

From the second congruence equation in Equation (4), we get

$$i = t(p-1), 1 \le t \le p^{\alpha-1}, \quad (5)$$

substituting Equation (5) into the first congruence equation in Equation (4), we get:

$$t(p-1)k \equiv 0(\bmod \varphi(p^\alpha)).$$

Note that $p^h \| k(h \ge 0)$, we write $k = p^h s, (s, p) = 1$, then $t(p-1)p^h s \equiv 0(\bmod \varphi(p^\alpha))$. Therefore, $p^{\alpha-1} \big| tp^h$. If $\alpha - 1 \le h$, then t has $p^{\alpha-1}$ solutions; if $\alpha - 1 > h$, $t \equiv 0(\bmod p^{\alpha-1-h})$, then t has p^h solutions.

Since the number of solutions of the first congruence equation in Equation (4) is $(k, \varphi(p^\alpha))$, then the number of solutions of system of congruencies Equation (3) is:

$$N = \begin{cases} (k, \varphi(p^\alpha)) - p^{\alpha-1}, \alpha - 1 \le h \\ (k, \varphi(p^\alpha)) - p^h, \alpha - 1 > h \end{cases}.$$

Lemma 5 Let p be an odd prime and k, α, i be integers with $\alpha \ge 1, i \ge 0, \alpha \ge i$ and $p^h \| k$. Define set:

$$E = \{(b,s) \big| (p,b) = (p,s) = (p, b-s) = 1, b^k - s^k \equiv 0(\bmod p^i)\},$$

where b, s run through a reduced residue system $\bmod p^\alpha$, then the values $b - s$ of set E takes all the values of the reduced residue system mod p^α, A times, where:

$$A = \begin{cases} p^{\alpha-i} A', i > 0 \\ p^{\alpha-1}(p-2), i = 0 \end{cases},$$

$$A' = \begin{cases} (k, \varphi(p^i)) - p^{i-1}, i - 1 \le h \\ (k, \varphi(p^i)) - p^h, i - 1 > h \end{cases}.$$

Proof We know that (b, s) of set E satisfies the following system of congruencies:

$$\begin{cases} b^k \equiv s^k (\bmod p^i) \\ b \not\equiv s(\bmod p) \end{cases}, \quad (6)$$

where b, s run through a reduced residue system $\bmod p^\alpha$

It is very clear that Equation (6) equivalents to the system of congruencies:

$$\begin{cases} (b\bar{s})^k \equiv 1(\bmod p^i) \\ b\bar{s} \not\equiv 1(\bmod p) \end{cases}. \quad (7)$$

If $i > 0$, by Lemma 4, we know the number of solutions of $b\bar{s}$ modulo p^i of (7) is

$$A' = \begin{cases} (k, \varphi(p^i)) - p^{i-1}, i - 1 \le h \\ (k, \varphi(p^i)) - p^h, i - 1 > h \end{cases}.$$

If $i = 0$, then the number of solutions of $b\bar{s}$ modulo p of Equation (7) is $p - 2$.

From the above two cases, we know the number of solutions of $b\bar{s}$ modulo p^α of Equation (6) is:

$$A = \begin{cases} p^{\alpha-i} A', i > 0 \\ p^{\alpha-1}(p-2), i = 0 \end{cases}.$$

Now let $a_1, \cdots, a_A (\bmod p^\alpha)$ be the solutions of $b\bar{s}$ modulo p^α. Fixing s in a reduced residue system modulo p^α, then:

$$b\bar{s} \equiv a_1, \cdots a_A (\bmod p^\alpha),$$

$$b - s \equiv (a_1 - 1)s, (a_2 - 1)s \cdots, (a_A - 1)s \ (\bmod p^\alpha).$$

Now let s run through a reduced residue system modulo p^α, then:

$$b_1 - s_1 \equiv (a_1 - 1)s_1, (a_2 - 1)s_1, \cdots, (a_A - 1)s_1 \ (\bmod p^\alpha),$$

$$b_2 - s_2 \equiv (a_1 - 1)s_2, (a_2 - 1)s_2, \cdots, (a_A - 1)s_2 \ (\bmod p^\alpha),$$

$\dots,$

$b_{\phi(p^\alpha)} - s_{\phi(p^\alpha)} \equiv$

$(a_1-1)s_{\phi(p^\alpha)}, (a_2-1)s_{\phi(p^\alpha)}, \cdots, (a_A-1)s_{\phi(p^\alpha)} (\bmod p^\alpha),$

$\{b-s\} =$

$\bigcup_{i=1}^{A} \{(a_i-1)s \mid \forall s \text{ in the reduced residue system } (\bmod p^\alpha)\}$

Thus, proves Lemma 5.

Lemma 6 Let p be an odd prime and i,t be integers such that $i \ge 1, t \ge 2,$ then we have:

$V_p\left(p^{it}C_k^t\right) > V_p\left(p^iC_k^1\right),$

where $V_p(\cdot)$ denotes the standard p-adic valuation.

Proof: We know:

$$V_p\left(p^{it}C_k^t\right) - V_p\left(p^iC_k^1\right) = it - i + V_p\left(C_k^t\right) - V_p\left(C_k^1\right) =$$
$$it - i + V_p\left(\frac{(k-1)\cdots(k-t+1)}{t!}\right) =$$
$$it - i + V_p\left((k-1)\cdots(k-t+1)\right) - V_p\left(t!\right) \ge$$
$$it - i - V_p\left(t!\right) = it - i - \left(\left[\frac{t}{p}\right] + \left[\frac{t}{p^2}\right] + \cdots\right) \ge$$
$$i(t-1) - \frac{t}{p-1} \ge t - 1 - \frac{t}{p-1} \ge \left(\frac{p-2}{p-1}\right)t - 1$$

If $p > 3$ or $p = 3$ with $t \ge 3,$ it is obviously that $V_p\left(p^{it}C_k^t\right) > V_p\left(p^iC_k^1\right).$

If $p = 3$ with $t = 2$, then

$V_p\left(p^{it}C_k^t\right) - V_p\left(p^iC_k^1\right) = i + V_3\left(C_k^2\right) - V_3\left(C_k^1\right) \ge 1.$

That completes the proof of Lemma 6.

Lemma 7 Let p be an odd prime with $(b,p) = (s,p) = 1$ and $p^i \parallel b - s (i \ge 1)$, let k, i be integers such that $i \ge 1,$ $k > 1$ and $p^h \parallel k$, then we have $p^{i+h} \parallel b^k - s^k$.

Proof: Let $b - s = vp^i, (p,v) = 1$, then:

$$b^k - s^k = (s + vp^i)^k - s^k =$$
$$C_k^1 s^{k-1} vp^i + C_k^2 s^{k-2}\left(vp^i\right)^2 + \cdots + C_k^k\left(vp^i\right)^k = \quad (8)$$
$$p^i C_k^1 s^{k-1} v + p^{2i} C_k^2 s^{k-2} v^2 + \cdots + p^{ik} C_k^k v^k$$

From Lemma 6, we know if $i \ge 1,\ t \ge 2,$ then $V_p\left(p^{it}C_k^t\right) > V_p\left(p^iC_k^1\right).$

Note that $p^h \parallel k, (v,p) = (s,p) = 1,$ therefore: $p^{i+h} \parallel b^k - s^k$.

Lemma 8 Let p be an odd prime with $(p,n) = 1$ and $k \ge 2, \alpha \ge 2$ be positive integers with $p \mid k.$ Define:

$$U_2(k;p^\alpha) = \sum_{i=1}^{\alpha-1} \sideset{}{'}\sum_{c=1}^{p^\alpha} \sideset{}{'}\sum_{b=1}^{p^\alpha} \sideset{}{'}\sum_{\substack{s=1 \\ (c^k-1)(b^k-s^k)\equiv 0 (\bmod p^\alpha) \\ p^i \| (c-1)(b-s)}}^{p^\alpha} e\left(\frac{n(c-1)(b-s)}{p^\alpha}\right),$$

then:

$U_2(k;p^\alpha) = -p^{2\alpha-2}(p-1)[2(p-2) + (\alpha-2)(p-1)]$.

Proof: Let:

$$U_{2i}(k;p^\alpha) = \sideset{}{'}\sum_{c=1}^{p^\alpha} \sideset{}{'}\sum_{b=1}^{p^\alpha} \sideset{}{'}\sum_{\substack{s=1 \\ (c^k-1)(b^k-s^k)\equiv 0 (\bmod p^\alpha) \\ p^i \| (c-1)(b-s)}}^{p^\alpha} e\left(\frac{n(c-1)(b-s)}{p^\alpha}\right),$$

then we have $U_2(k;p^\alpha) = \sum_{i=1}^{\alpha-1} U_{2i}(k;p^\alpha)$.

Now we split the sum $U_{2i}(k;p^\alpha)$ into three terms:

$$U_{2i}^1(k;p^\alpha) = \sideset{}{'}\sum_{c=1}^{p^\alpha} \sideset{}{'}\sum_{b=1}^{p^\alpha} \sideset{}{'}\sum_{\substack{s=1 \\ (c^k-1)(b^k-s^k)\equiv 0 (\bmod p^\alpha) \\ p\nmid(c-1),\, p^i \| (b-s)}}^{p^\alpha} e\left(\frac{n(c-1)(b-s)}{p^\alpha}\right),$$

$$U_{2i}^2(k;p^\alpha) = \sum_{\beta=1}^{i-1} \sideset{}{'}\sum_{c=1}^{p^\alpha} \sideset{}{'}\sum_{b=1}^{p^\alpha} \sideset{}{'}\sum_{\substack{s=1 \\ (c^k-1)(b^k-s^k)\equiv 0 (\bmod p^\alpha) \\ p^\beta \| (c-1),\, p^{i-\beta} \| (b-s)}}^{p^\alpha} e\left(\frac{n(c-1)(b-s)}{p^\alpha}\right),$$

$$U_{2i}^3(k;p^\alpha) = \sideset{}{'}\sum_{c=1}^{p^\alpha} \sideset{}{'}\sum_{b=1}^{p^\alpha} \sideset{}{'}\sum_{\substack{s=1 \\ (c^k-1)(b^k-s^k)\equiv 0 (\bmod p^\alpha) \\ p\nmid(b-s),\, p^i \| (c-1)}}^{p^\alpha} e\left(\frac{n(c-1)(b-s)}{p^\alpha}\right),$$

thus:

$$U_{2i}(k;p^\alpha) = U_{2i}^1(k;p^\alpha) + U_{2i}^2(k;p^\alpha) + U_{2i}^3(k;p^\alpha). \quad (9)$$

Let h denote the number $p^h \parallel k$, from the condition $p \mid k$ we immediately get $h \ge 1$.

1) For $\alpha = 2$, we have $i = 1$ and therefore: $U_{21}^2(k;p^2) = 0$.

From Lemma 7, if $p \parallel b - s,$ then $p^{h+1} \parallel b^k - s^k,$ so

$$U_{21}^1(k,p^2) = \sideset{}{'}\sum_{c=1}^{p^2} \sideset{}{'}\sum_{b=1}^{p^2} \sideset{}{'}\sum_{\substack{s=1 \\ (c^k-1)(b^k-s^k)\equiv 0 (\bmod p^2) \\ p\nmid(c-1),\, p\|(b-s)}}^{p^2} e\left(\frac{n(c-1)(b-s)}{p^2}\right) =$$

$$\sideset{}{'}\sum_{\substack{c=1 \\ p\nmid(c-1)}}^{p^2} \sideset{}{'}\sum_{s=1}^{p^2} \sideset{}{'}\sum_{v=1}^{p} e\left(\frac{n(c-1)v}{p}\right) = \sideset{}{'}\sum_{\substack{c=1 \\ p\nmid(c-1)}}^{p^2} \sideset{}{'}\sum_{s=1}^{p^2} (-1) =$$

$$-p^2(p-1)(p-2).$$

By Lemma 7, we know if $p \parallel c - 1,$ then $p^{h+1} \parallel c^k - 1,$ so:

$$U_{21}^3(k;p^2) = \sideset{}{'}\sum_{c=1}^{p^2} \sideset{}{'}\sum_{b=1}^{p^2} \sideset{}{'}\sum_{\substack{s=1 \\ (c^k-1)(b^k-s^k)\equiv 0 (\bmod p^2) \\ p\nmid(b-s),\, p\|(c-1)}}^{p^2} e\left(\frac{n(c-1)(b-s)}{p^2}\right) =$$

$$\sideset{}{'}\sum_{t=1}^{p} \sideset{}{'}\sum_{\substack{b=1 \\ p\nmid b-s}}^{p^2} \sideset{}{'}\sum_{s=1}^{p^2} e\left(\frac{nt(b-s)}{p}\right) = p^2 \sideset{}{'}\sum_{t=1}^{p} \sideset{}{'}\sum_{\substack{b=1 \\ p\nmid b-s}}^{p} \sideset{}{'}\sum_{s=1}^{p} e\left(\frac{nt(b-s)}{p}\right).$$

By using Lemmas 1 and 5, we have:

$$U_{21}^3(k;p^2) = -p^2 \sum_{t=1}^{p}{}' (p-2) = -p^2(p-1)(p-2).$$

Then:

$$U_{21}(k;p^2) = U_{21}^1(k;p^2) + U_{21}^3(k;p^2) = -2p^2(p-1)(p-2),$$

$$U_2(k;p^2) = U_{21}(k;p^2) = -2p^2(p-1)(p-2).$$

2) Now we suppose $\alpha \ge 3$, first we consider:

$$U_{2i}^1(k;p^\alpha) = \sum_{\substack{c=1 \\ (c^k-1)(b^k-s^k)\equiv 0(\mathrm{mod}\, p^\alpha) \\ p\nmid(c-1),\, p^i \| (b-s)}}^{p^\alpha}{}' \sum_{b=1}^{p^\alpha}{}' \sum_{s=1}^{p^\alpha}{}' e\left(\frac{n(c-1)(b-s)}{p^\alpha}\right).$$

By using Lemma 7, we know if $p^i \| b-s$, then $p^{i+h} \| b^k - s^k$, if $\alpha - i \ge h+1$, then the congruence equation $(c^k-1)(b^k-s^k) \equiv 0(\mathrm{mod}\, p^\alpha)$ equivalents to the congruence $c^k - 1 \equiv 0(\mathrm{mod}\, p^{\alpha-i-h})$; if $\alpha - i \le h$, the congruence $(c^k-1)(b^k-s^k) \equiv 0(\mathrm{mod}\, p^\alpha)$ obviously holds.

Case 1 If $\alpha - i \le h$, then:

$$U_{2i}^1(k;p^\alpha) = \sum_{\substack{c=1 \\ p\nmid(c-1)}}^{p^\alpha}{}' \sum_{v=1}^{p^{\alpha-i}}{}' \sum_{s=1}^{p^\alpha}{}' e\left(\frac{n(c-1)v}{p^{\alpha-i}}\right) =$$

$$\varphi(p^\alpha) \sum_{\substack{c=1 \\ p\nmid(c-1)}}^{p^\alpha}{}' \sum_{v=1}^{p^{\alpha-i}}{}' e\left(\frac{n(c-1)v}{p^{\alpha-i}}\right) =$$

$$\varphi(p^\alpha) p^{\alpha-1}[\varphi(p)-1] \sum_{v=1}^{p^{\alpha-i}}{}' e\left(\frac{n(c-1)v}{p^{\alpha-i}}\right) =$$

$$\begin{cases} 0, 2 \le \alpha - i \le h \\ -p^{2\alpha-2}(p-1)(p-2), 1 = \alpha - i \le h \end{cases}.$$

Case 2 If $\alpha - i \ge h+1$, then

$$U_{2i}^1(k;p^\alpha) = \sum_{\substack{c=1 \\ c^k-1\equiv 0(\mathrm{mod}\, p^{\alpha-i-h}) \\ p\nmid(c-1)}}^{p^\alpha}{}' \sum_{s=1}^{p^\alpha}{}' \sum_{v=1}^{p^{\alpha-i}}{}' e\left(\frac{n(c-1)v}{p^{\alpha-i}}\right) = 0.$$

From the above two cases, we get

$$U_{2i}^1(k;p^\alpha) = \begin{cases} 0, 1 \le i \le \alpha - 2 \\ -p^{2\alpha-2}(p-1)(p-2), i = \alpha - 1 \end{cases}.$$

Similarly to the method of computing $U_{2i}^1(k;p^\alpha)$, we get:

$$U_{2i}^3(k;p^\alpha) = \sum_{\substack{c=1 \\ (c^k-1)(b^k-s^k)\equiv 0(\mathrm{mod}\, p^\alpha) \\ p\nmid(b-s),\, p^i \| (c-1)}}^{p^\alpha}{}' \sum_{b=1}^{p^\alpha}{}' \sum_{s=1}^{p^\alpha}{}' e\left(\frac{n(c-1)(b-s)}{p^\alpha}\right) =,$$

$$\begin{cases} 0, 1 \le i \le \alpha - 2 \\ -p^{2\alpha-2}(p-1)(p-2), i = \alpha - 1 \end{cases}.$$

At last, we compute:

$$U_{2i}^2(k;p^\alpha) = \sum_{\beta=1}^{i-1} \sum_{\substack{c=1 \\ (c^k-1)(b^k-s^k)\equiv 0(\mathrm{mod}\, p^\alpha) \\ p^\beta \| (c-1),\, p^{i-\beta} \| (b-s)}}^{p^\alpha}{}' \sum_{b=1}^{p^\alpha}{}' \sum_{s=1}^{p^\alpha}{}' e\left(\frac{n(c-1)(b-s)}{p^\alpha}\right).$$

By Lemma 7, we know if $p^\beta \| (c-1)$ and $p^{i-\beta} \| (b-s)$, then $p^{\beta+h} \| c^k - 1$, $p^{i-\beta+h} \| b^k - s^k$ and $p^{i+2h} \| (c^k-1)(b^k-s^k)$. If $i + 2h \ge \alpha$, then the equation $(c^k-1)(b^k-s^k) \equiv 0(\mathrm{mod}\, p^\alpha)$ obviously holds. If $i + 2h \le \alpha - 1$, surely, the congruence equation $(c^k-1)(b^k-s^k) \equiv 0(\mathrm{mod}\, p^\alpha)$ cannot hold.

Case 1 If $\alpha - i \le 2h$, then:

$$U_{2i}^2(k;p^\alpha) = \sum_{\substack{\beta=1 \\ p^\beta \| (c-1),\, p^{i-\beta} \| b-s}}^{i-1} \sum_{s=1}^{p^\alpha}{}' \sum_{c=1}^{p^\alpha}{}' \sum_{b=1}^{p^\alpha}{}' e\left(\frac{n(c-1)(b-s)}{p^\alpha}\right) =$$

$$\sum_{\beta=1}^{i-1} \sum_{s=1}^{p^\alpha}{}' \sum_{u=1}^{p^{\alpha-\beta}}{}' \sum_{v=1}^{p^{\alpha+\beta-i}}{}' e\left(\frac{nuv}{p^{\alpha-i}}\right) =$$

$$\sum_{\beta=1}^{i-1} \sum_{s=1}^{p^\alpha}{}' \sum_{u=1}^{p^{\alpha-\beta}}{}' p^\beta \sum_{v=1}^{p^{\alpha-i}}{}' e\left(\frac{nuv}{p^{\alpha-i}}\right) =$$

$$\varphi(p^\alpha) \sum_{\beta=1}^{i-1} p^\beta \sum_{u=1}^{p^{\alpha-\beta}}{}' \sum_{v=1}^{p^{\alpha-i}}{}' e\left(\frac{nuv}{p^{\alpha-i}}\right) =$$

$$\begin{cases} 0, 2 \le \alpha - i \le 2h \\ -(\alpha-2)p^{2\alpha-2}(p-1)^2, \alpha - i = 1 \end{cases}$$

Case 2 If $\alpha - i \ge 2h+1$, then

$$U_{2i}^2(k;p^\alpha) = 0.$$

Therefore:

$$U_{2i}^2(k;p^\alpha) = \begin{cases} 0, 1 \le i \le \alpha - 2 \\ -(\alpha-2)p^{2\alpha-2}(p-1)^2, i = \alpha - 1 \end{cases}.$$

Using Equation (9), we immediately get:

$$U_{2i}(k;p^\alpha) = \begin{cases} 0, i \le \alpha - 2 \\ -p^{2\alpha-2}(p-1)[2(p-2)+(\alpha-2)(p-1)], i = \alpha - 1 \end{cases}$$

Therefore,

$$U_2(k;p^\alpha)=\sum_{i=1}^{\alpha-1}U_{2i}(k;p^\alpha)=$$
$$-p^{2\alpha-2}(p-1)[2(p-2)+(\alpha-2)(p-1)].$$

In conclusion, we have if $\alpha\ge 2$, then

$$U_2(k;p^\alpha)=-p^{2\alpha-2}(p-1)[2(p-2)+(\alpha-2)(p-1)].$$

Lemma 9 Let p be a prime with $(p,n)=1$, k,α be positive integers such that $k>1$ and $d=(k,p-1)$.

Define

$$U_3(k;p^\alpha)=\sum_{\substack{c=1\\(c^k-1)(b^k-s^k)\equiv 0(\mathrm{mod}\,p^\alpha)\\p\nmid(c-1)(b-s)}}^{p^\alpha}{}'\sum_{b=1}^{p^\alpha}{}'\sum_{s=1}^{p^\alpha}{}'\ e\left(\frac{n(c-1)(b-s)}{p^\alpha}\right),$$

then

$$U_3(k;p^\alpha)=\begin{cases}-2(p-1)(d-1)+d^2-1,\alpha=1,\\0, \qquad\qquad\qquad\qquad \alpha\ge 2.\end{cases}$$

Proof: 1) For $\alpha=1$, we split the sum $U_3(k;p)$ into two terms:

$$U_3(k;p)=\sum_{\substack{c=1\\(c^k-1)(b^k-s^k)\equiv 0(\mathrm{mod}\,p)\\p\nmid(c-1)(b-s)}}^{p}{}'\sum_{b=1}^{p}{}'\sum_{s=1}^{p}{}'\ e\left(\frac{n(c-1)(b-s)}{p}\right)=$$
$$\sum_{\substack{c=1\\p\nmid(c-1)(b-s)\\p|(c^k-1)}}^{p}{}'\sum_{b=1}^{p}{}'\sum_{s=1}^{p}{}'\ e\left(\frac{n(c-1)(b-s)}{p}\right)+$$
$$\sum_{\substack{c=1\\p\nmid(c^k-1),\,p|(b^k-s^k)\\p\nmid(c-1)(b-s)}}^{p}{}'\sum_{b=1}^{p}{}'\sum_{s=1}^{p}{}'\ e\left(\frac{n(c-1)(b-s)}{p}\right)=$$
$$U_{31}(k;p)+U_{32}(k;p)$$

First we compute $U_{31}(k;p)$,

$$U_{31}(k;p)=\sum_{\substack{c=1\\p\nmid(c-1)(b-s)\\p|(c^k-1)}}^{p}{}'\sum_{b=1}^{p}{}'\sum_{s=1}^{p}{}'\ e\left(\frac{n(c-1)(b-s)}{p}\right)=$$
$$\sum_{\substack{c=1\\p\nmid(c-1)\\p|(c^k-1)}}^{p}{}'\ \sum_{\substack{b=1\\p\nmid(b-s)}}^{p}{}'\sum_{s=1}^{p}{}'\ e\left(\frac{n(c-1)(b-s)}{p}\right).$$

By Lemma 5, we know $b-s$ takes all the values of the reduced residue system mod p, $p-2$ times. With the properties of Ramanujan sum (see Lemma 1), we have:

$$U_{31}(k;p)=-\sum_{\substack{c=1\\p\nmid(c-1)\\p|(c^k-1)}}^{p}{}'(p-2)=-(p-2)(d-1).$$

Now we consider:

$$U_{32}(k;p)=\sum_{\substack{c=1\\p\nmid(c^k-1),\,b^k-s^k\equiv 0(\mathrm{mod}\,p)\\p\nmid(c-1),\,p\nmid b-s}}^{p}{}'\sum_{b=1}^{p}{}'\sum_{s=1}^{p}{}'\ e\left(\frac{n(c-1)(b-s)}{p}\right).$$

From Lemma 5, we know $b-s$ takes all the values of the reduced residue system mod p, $d-1$ times, then:

$$U_{32}(k;p)=\sum_{\substack{c=1\\p\nmid(c-1)\\p\nmid(c^k-1)}}^{p}{}'(-1)(d-1)=(-1)(p-1-d)(d-1).$$

Therefore:

$$U_3(k;p)=U_{31}(k;p)+U_{32}(k;p)=-(d-1)(2p-d-3).$$

2) For $\alpha\ge 2$,

$$U_3(k;p^\alpha)=\sum_{\substack{c=1\\(c^k-1)(b^k-s^k)\equiv 0(\mathrm{mod}\,p)\\p\nmid(c-1)(b-s)}}^{p}{}'\sum_{b=1}^{p}{}'\sum_{s=1}^{p}{}'\ e\left(\frac{n(c-1)(b-s)}{p^\alpha}\right)=$$
$$\sum_{i=1}^{\alpha-1}\ \sum_{\substack{c=1\\p^i\|(c^k-1),\,b^k-s^k\equiv 0\left(\mathrm{mod}\,p^{\alpha-i}\right)\\p\nmid(c-1),\quad p\nmid(b-s)}}^{p^\alpha}{}'\sum_{b=1}^{p^\alpha}{}'\sum_{s=1}^{p^\alpha}{}'\ e\left(\frac{n(c-1)(b-s)}{p^\alpha}\right).$$

From Lemma 5, we know $b-s$ takes all the values of the reduced residue system mod p^α some times, then we have:

$$\sum_{\substack{b=1\\b^k-s^k\equiv 0\left(\mathrm{mod}\,p^{\alpha-i}\right)\\p\nmid(b-s)}}^{p^\alpha}{}'\sum_{s=1}^{p^\alpha}{}'\ e\left(\frac{n(c-1)(b-s)}{p^\alpha}\right)=0.$$

So:

$$U_3(k;p^\alpha)=0.$$

In conclusion, we have:

$$U_3(k;p^\alpha)=\begin{cases}-(d-1)(2p-d-3),\alpha=1\\0,\alpha\ge 2\end{cases}.$$

3 Proof of the Theorem 1

Now we prove Theorem 1.

Proof: We split the sum:

$$U(k;p^\alpha)=\sum_{\substack{c=1\\(c^k-1)(b^k-s^k)\equiv 0(\mathrm{mod}\,p^\alpha)}}^{p^\alpha}{}'\sum_{b=1}^{p^\alpha}{}'\sum_{s=1}^{p^\alpha}{}'\ e\left(\frac{n(c-1)(b-s)}{p^\alpha}\right)$$

into three terms:

$$U_1(k;p^\alpha)=\sum_{\substack{c=1\\p^\alpha|(c-1)(b-s)}}^{p^\alpha}{}'\sum_{b=1}^{p^\alpha}{}'\sum_{s=1}^{p^\alpha}{}'1,$$

$$U_2(k;p^\alpha)=\sum_{i=1}^{\alpha-1}\sum_{\substack{c=1 \\ (c^k-1)(b^k-s^k)\equiv 0(\mathrm{mod}\, p^\alpha) \\ p^i\|(c-1)(b-s)}}^{p^\alpha}{}'\sum_{b=1}^{p^\alpha}{}'\sum_{s=1}^{p^\alpha}{}' e\left(\frac{n(c-1)(b-s)}{p^\alpha}\right),$$

$$U_3(k;p^\alpha)=\sum_{\substack{c=1 \\ (c^k-1)(b^k-s^k)\equiv 0(\mathrm{mod}\, p^\alpha) \\ p\nmid(c-1)(b-s)}}^{p^\alpha}{}'\sum_{b=1}^{p^\alpha}{}'\sum_{s=1}^{p^\alpha}{}' e\left(\frac{n(c-1)(b-s)}{p^\alpha}\right),$$

Thus:

$$U(k;p^\alpha)=U_1(k;p^\alpha)+U_2(k;p^\alpha)+U_3(k;p^\alpha).$$

If $\alpha=1$, by Lemma 4, 8 and 9, we get

$$U(k;p)=U_1(k,;p)+U_3(k;p)=$$
$$(p-1)(2p-3)-[(k,p-1)-1)][2p-(k,p-1)-3]=$$
$$(p-1)(2p-3)-(d-1)(2p-d-3).$$

If $\alpha\ge 2$, by Lemma 4, 8 and 9, we get:

$$U(k;p^\alpha)=U_1(k;p^\alpha)+U_2(k;p^\alpha)+U_3(k;p^\alpha)=$$
$$(\alpha+1)\varphi^2(p^\alpha)-\varphi(p^\alpha)p^{\alpha-1}-p^{\alpha-1}\varphi(p^\alpha)[2(p-2)+$$
$$(\alpha-2)(p-1)]=\varphi(p^\alpha)p^\alpha = p^{2\alpha-1}(p-1).$$

Therefore:

$$U(k;p^\alpha)=\begin{cases}(p-1)(2p-3)-(d-1)(2p-d-3),\alpha=1\\ p^{2\alpha-1}(p-1),\alpha\ge 2\end{cases}.$$

From Lemma 4, we have:

$$M_k(p^\alpha)=$$
$$\begin{cases}p(p-1)^2[2p(p-d)-3p+d(d+2)](p^2-p-1),\alpha=1\\ p^{7\alpha-4}(p-1)^4,\alpha\ge 2\end{cases}.$$

Now we compute $\sum_{m=1}^{q}\sum_{\chi\,\mathrm{mod}\, q}\left|C(m,n,\chi,k,q)\right|^4$.

It is not hard to see that:

$$S(m,n,\chi,\chi',p^\alpha)=G(1,\chi')C(m,n,\chi\overline{\chi'},k,p^\alpha),$$

So:

$$M_k(p^\alpha)=\sum_{m=1}^{p^\alpha}\sum_{\chi\,\mathrm{mod}\, p^\alpha}\sum_{\chi'\,\mathrm{mod}\, p^\alpha}\left|S(m,n,\chi,\chi',p^\alpha)\right|^4=$$
$$\sum_{\chi'(\mathrm{mod}\, p^\alpha)}\left|G(1,\chi')\right|^4\sum_{m=1}^{p^\alpha}\sum_{\chi\,\mathrm{mod}\, p^\alpha}\left|C(m,n,\chi\overline{\chi'},k,p^\alpha)\right|^4=$$
$$\sum_{\chi'(\mathrm{mod}\, p^\alpha)}\left|G(1,\chi')\right|^4\sum_{m=1}^{p^\alpha}\sum_{\chi\,\mathrm{mod}\, p^\alpha}\left|C(m,n,\chi,k,p^\alpha)\right|^4.$$

From the proposition 3.1 in the Ref. [1], we have

$$M_k(p^\alpha)=\varphi(p^\alpha)\sum_{c=1}^{p^\alpha}{}'C_{p^\alpha}^2(c-1)\sum_{m=1}^{p^\alpha}\sum_{\chi\,\mathrm{mod}\, p^\alpha}\left|C(m,n,\chi,k,p^\alpha)\right|^4=$$
$$\sum_{m=1}^{p^\alpha}\sum_{\chi\,\mathrm{mod}\, p^\alpha}\left|C(m,n,\chi,k,p^\alpha)\right|^4\cdot\begin{cases}(p^2-p-1)(p-1),\alpha=1\\ p^{3\alpha-2}(p-1)^2,\alpha\ge 2\end{cases}.$$

From the above result, we have:

$$\sum_{m=1}^{p^\alpha}\sum_{\chi(\mathrm{mod}\, p^\alpha)}\left|C(m,n,\chi,k,p^\alpha)\right|^4=$$
$$\begin{cases}p(p-1)^3\left[2-\frac{2d-1}{p-1}+\frac{d^2-1}{(p-1)^2}\right],\alpha=1\\ p^{4\alpha-2}(p-1)^2,\alpha\ge 2\end{cases}$$

This completes the proof of Theorem 1.

From Theorem 1, Assumption 1, 2 and Lemma 2, we immediately get the Generalization of Theorem 1.

Generalization of Theorem 1 Let q be an odd integer with $q\ge 3$ and k be an integer with $k\ge 1$, then for any fixed positive integer n with $(n,q)=1$, we have:

$$M_k(q)=\sum_{m=1}^{q}\sum_{\chi(\mathrm{mod}\, q)}\sum_{\chi'(\mathrm{mod}\, q)}\left|S(m,n,\chi,\chi',q)\right|^4=\prod_{p\|q}p(p-1)^2(p^2-p-1)\{2p[p-(k,p-1)]-3p+(k,p-1)[(k,p-1)+2]\}\cdot$$
$$\prod_{\substack{p^2|q\\(k,p)=p}}p^{7\alpha-4}(p-1)^4\cdot\prod_{\substack{p^2|q\\(k,p)=1}}p^{7\alpha-5}(p-1)^4\{(\alpha+1)(p-1)-[2(k,p-1)-1]\}.$$

and

$$\sum_{m=1}^{q}\sum_{\chi\,\mathrm{mod}\, q}\left|C(m,n,\chi,k,q)\right|^4=\prod_{p\|q}p(p-1)^3\left[2-\frac{2(k,p-1)-1}{p-1}+\frac{(k,p-1)^2-1}{(p-1)^2}\right]$$
$$\cdot\prod_{\substack{p^2|q\\(k,p)=1}}p^{4\alpha-3}(p-1)^3\left[\alpha+1-\frac{(k,p-1)-1}{p-1}\right]\cdot\prod_{\substack{p^2|q\\(k,p)=p}}p^{4\alpha-2}(p-1)^2,$$

where $\prod_{p^\alpha\|q}$ denotes the product over all prime p of q with $p^\alpha\mid q$ and $p^{\alpha+1}\nmid q$.

Acknowledgments

This work was supported in part by NSF grants of Navy University of Engineering (No. HGDQNEQJJ13001) and

NSF grants of Hubei province (Grant No. 2011CDB081). The authors express their gratitude to the editor and reviewer for their helpful and detailed comments.

References

[1] Calderón C, de Velasco M J, Zarate M. J 2011 An explicit formula for the fourth moment of certain exponential sums *Acta Mathematica Hungarican* **130**(3) 203-22

[2] Xu Z F, Zhang T P, Zhang W P 2007 On the mean value of the two-term exponential sums with Dirichlet characters *Journal of Number Theory* **123**(2) 352-62

[3] Weil A 1948 On some exponential sums *Proceedings of the National Academy of Sciences of the United States of America* **34** 204-7

[4] Cochrane T, Zheng Z Y 2000 Bound for certain exponential sums *The Asian Journal of Mathematics* **4** 757-73

[5] Liu H N 2008 Mean value of mixed exponential sums *Proceedings of American Mathematical Society* **136**(4) 1193-203

[6] Wang T T, Zhang W P 2011 Mean value of the mixed fourth and Sixth exponential sums *Science China (mathematical edition)* **41**(3) 265-270 *(in Chinese)*

[7] Hua L K 1979 Introduction to number theory *Science Press: Beijing China*

Authors

Xiaochuan Ai, June 1978, China.

Current position, grades: doctoral student at Wuhan University, China. Lecturer at the School of Science, Navy University of Engineering, China.
University studies: master's degree at the School of Mathematics and Statistics from Wuhan University, China in 2006.

Jianhua Chen, January 1963, China.

Current position, grades: professor and doctoral tutor at the School of Mathematics and Statistics, Wuhan University, China.
Scientific interests: number theory, cryptography and information safety.

Hua Chen, October 1981, China.

Current position, grades: lecturer at the School of Science, Hubei University of Technology, China.
University studies: PhD degree at the School of Mathematics and Statistics from Wuhan University, China in 2012.
Scientific interests: number theory, cryptography and information safety.

Silan Zhang, October 1980, China.

Current position, grades: doctoral student at Wuhan University, China. Lecturer at the College of Science, Huazhong Agricultural University, China.
University studies: master's degree at the School of Mathematics and Statistics from Wuhan University, China in 2006.