Hua CHEN[1,2] ,Jianhua CHEN[2], Guangxing CAI[1] , Aihua LUO[3*]

School of science, Hubei University of Technology(1),School of mathematics and Statistics, Wuhan University (2), School of Mathematics and Statistics, South-Central University for Nationalities(3)

Explicit Formulas for the Fourth Moment of Exponential Sums and Dirichlet Character Sums

Abstract. Exponential sums and Dirichlet character sums have important applications in electronic science and technology, such as e-commerce, e-government and so on. With elementary method, the computation problem of the fourth power mean $\sum_{m=1}^{q}\sum_{\chi \bmod q}|\sum_{a=1}^{q}{}'\chi(a)e(\frac{ma^k+na}{q})|^4$ is studied, where $e(y)=e^{2\pi iy}$, χ is a Dirichlet character modulo q and $\sum_{a=1}^{q}{}'$ denotes the summation over all a with $(a,q)=1$. A new proof is proposed and some interesting computational formula and transformation formula are obtained.

Streszczenie. *W artykule przedstawiono zagadnienie rozwiązywania wyrażenia zawierającego sumy wykładnicze oraz sumy operatorów Dirichleta. Zaproponowano nowy dowód, formułę obliczeń oraz formułę transformacji. (**Funkcja jawna dla czwartej potęgi sum wykładniczych i sum operatora Dirichleta**).*

Keywords: exponential sums; Dirichlet character; fourth power value; computational formula
Słowa kluczowe: sumy wykładnicze, operator Dirichleta, wartość czwartej potęgi, formuła obliczeniowa.

Introduction

For integers q,m,n,k with $q\geq 3,\ k\geq 2$, we define the two-term exponential sums $C(m,n,k;q)=\sum_{a=1}^{q}{}'e(\frac{ma^k+na}{q})$ and define the two-term exponential sums with Dirichlet character $C(m,n,k,\chi;q)=\sum_{a=1}^{q}{}'\chi(a)e(\frac{ma^k+na}{q})$. As we all know, both Exponential sums and Dirichlet character sums have important applications. For example, Exponential sums originally arose in connection with famous Waring's problem. Dirichlet character sums have close relation with elliptic curve cryptography (ECC), which has important applications in electronic science and technology, such as e-commerce, e-government and so on. The value of exponential sums or Dirichlet character sums is irregular and its computation is very difficult. However, the mixed mean value of exponential sums with Dirichlet character owns excellent arithmetical properties. The researchers tried to study the former by discussing the latter. Recently, on the premise of $(k,p)=1$, using the analytic method ,Xu[3] have proved

(1) $$\sum_{m=1}^{p}\sum_{\chi \bmod p}|c(m,n,k,\chi,p)|^4=(p-1)^3p(2-\frac{2(k,p-1)-1}{p-1}+\frac{(k,p-1)^2-1}{(p-1)^2}).$$

The purpose of this paper is using the elementary method to make researches into the computational problem of $\sum_{m=1}^{q}\sum_{\chi \bmod q}|c(m,n,k,\chi;q)|^4$ and we will prove the following.

Theorem. Let p be an odd prime. For each fixed positive integer n,k, we have

(2) $$\sum_{m=1}^{p}\sum_{\chi \bmod p}|c(m,n,k,\chi;p)|^4=\begin{cases}(p-1)^3p+(p-1)\sum_{a=2}^{p-1}\sum_{m=1}^{p}|C(m,n,k;p)|^2,(k,p-1)=1\\(p-1)^3p+(p-1)p|\sum_{b=1}^{p-1}e(\frac{nb(p-2)}{p})|^2+(p-1)\sum_{a=2}^{p-2}\sum_{m=1}^{p}|C(m,n,k;p)|^2,k=2\end{cases}$$

Moreover, if $(n,p)=1$, we have

(3) $$\sum_{m=1}^{p}\sum_{\chi \bmod p}|c(m,n,k,\chi,p)|^4=\begin{cases}(p-1)^2p(2p-3), & (k,p-1)=1\\(p-1)p(2p^2-7p+8), & k=2\end{cases}$$

Remark: From Xu's work[3] , we could obtain a proposition as follows:

Proposition Let p be an odd prime. Then for any fixed positive integer n with $(n,p)=1$, we have

(4) $$\sum_{m=1}^{p}\sum_{\chi \bmod p}|c(m,n,k,\chi,p)|^4=\begin{cases}(p-1)^2p(2p-3), & (k,p(p-1))=1\\(p-1)p(2p^2-7p+8), & k=2\end{cases}$$

Obviously, Xu's result is established under a stronger assumption condition. From this point , the method in this paper is better.

Generalization of Theorem. Let $q=p_1p_2\cdots p_t$ be a positive integer with $q\geq 3$. Then for arbitrary integers n,k with $(n,q)=1$, we have

(5) $$\sum_{m=1}^{q}\sum_{\chi \bmod q}|c(m,n,k,\chi;q)|^4=\begin{cases}q\varphi^2(q)\prod_{p\|q}(2p-3), & (k,\varphi(q))=1\\q\varphi^2(q)\prod_{p\|q}(2p^2-7p+8), & k=2\end{cases}$$

where $\varphi(q)$ is a Euler function, and $\prod_{p\|q}$ denotes the product over all prime p of q with $p\mid q$ and $p^2\nmid q$.

Preliminaries

To prove Theorem and its generalization, the following lemmas will be useful.

Lemma 1.Let p be an odd prime. For each fixed positive integer n,k with $(n,q)=1$, we have

(1) $$\sum_{m=1}^{p}|C(m,n,k;p)|^2=\begin{cases}p^2-p, & (k,p-1)=1\\p^2-2p, & k=2\end{cases}$$

Proof. Let r be arbitrary integer with $(r,p)=1$, then $(\overline{r},p)=1$, where $\overline{r}$ denotes the solution of congruences equation $xr\equiv 1(\bmod p)$. From the properties of reduced systems, we have

$$\sum_{m=1}^{p}|C(m,n,k;p)|^2=\sum_{m=1}^{p}|\sum_{a=1}^{p}{}'e(\frac{ma^k+na}{p})|^2$$
$$=\sum_{m=1}^{p}|\sum_{a=1}^{p-1}e(\frac{m\overline{r}^{k}a^k+na}{p})|^2=\frac{1}{p-1}\sum_{r=1}^{p-1}\sum_{m=1}^{p}|\sum_{a=1}^{p-1}e(\frac{ma^k+nra}{p})|^2$$
$$=\frac{1}{p-1}\sum_{r=1}^{p}\sum_{m=1}^{p}|\sum_{a=1}^{p-1}e(\frac{ma^k+nra}{p})|^2-\frac{1}{p-1}\sum_{m=1}^{p}|\sum_{a=1}^{p-1}e(\frac{ma^k}{p})|^2$$
$$=C_1-C_2$$

First, we compute C_1.

$$C_1=\frac{1}{p-1}\sum_{r=1}^{p}\sum_{m=1}^{p}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}e(\frac{m(a^k-b^k)+nr(a-b)}{p})$$
$$=\frac{1}{p-1}[p^2(p-1)+\sum_{r=1}^{p}\sum_{m=1}^{p}\sum_{a=2}^{p-1}\sum_{b=1}^{p-1}e(\frac{mb^k(a^k-1)+nrb(a-1)}{p})]$$
$$=p^2+\frac{1}{p-1}\sum_{r=1}^{p}\sum_{m=1}^{p}\sum_{a=2}^{p-1}\sum_{b=1}^{p-1}e(\frac{m(b\overline{(a-1)})^k(a^k-1)+nrb\overline{(a-1)}(a-1)}{p})]$$
$$=p^2+\frac{1}{p-1}\sum_{r=1}^{p}\sum_{b=1}^{p-1}e(\frac{nrb}{p})\sum_{m=1}^{p}\sum_{a=2}^{p-1}e(\frac{m(b\overline{(a-1)})^k(a^k-1)}{p})]$$

From the trigonometrical identity , we have

$$\sum_{r=1}^{p}\sum_{b=1}^{p-1}e(\frac{nrb}{p})=0\ ,$$

so $C_1=p^2$.

Then we compute C_2 from two situations.

Firstly, if $(k,p-1)=1$, then

$$C_2=\frac{1}{p-1}\sum_{m=1}^{p}|\sum_{a=1}^{p-1}e(\frac{ma^k}{p})|^2=\frac{1}{p-1}\sum_{m=1}^{p}|\sum_{a=1}^{p-1}e(\frac{ma}{p})|^2$$
$$=\frac{1}{p-1}[(p-1)^2+\sum_{m=1}^{p-1}|\sum_{a=1}^{p-1}e(\frac{ma}{p})|^2]=p$$

Secondly, if $k=2$,then

$$C_2=\frac{1}{p-1}\sum_{m=1}^{p}|\sum_{a=1}^{p-1}e(\frac{ma^2}{p})|^2$$
$$=\frac{1}{p-1}\sum_{m=1}^{p-1}|\sum_{a=1}^{p-1}(1+\left(\frac{a}{p}\right))e(\frac{ma}{p})|^2+(p-1)$$
$$=\frac{1}{p-1}\sum_{m=1}^{p-1}|\sum_{a=1}^{p-1}e(\frac{ma}{p})+\left(\frac{m}{p}\right)\tau(\chi)|^2+(p-1)$$

where $\left(\frac{a}{p}\right)$ denotes Legendre symbol and

$$\tau(\chi)=\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)e\left(\frac{a}{p}\right).$$

Note that

$$\tau(\chi)=\begin{cases}\sqrt{p}, & p\equiv 1\bmod 4\\ i\sqrt{p}, & p\equiv 3\bmod 4\end{cases},$$

so $C_2=2p$. This proves Lemma1.

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 and let $\chi=\chi_1\chi_2\cdots\chi_t \bmod q$ such that $\chi_j \bmod p_j^{\alpha_j}$ $(j=1,2,\cdots,t)$ .Then we have

(2) $$\left|\sum_{a=1}^{q}{}'\chi(a)e(\frac{ma^k+na}{q})\right|=\prod_{j=1}^{t}\left|\sum_{a_j=1}^{p_j^{\alpha_j}}{}'\chi_j(\frac{q}{p_j^{\alpha_j}}a_j)e(\frac{m(\frac{q}{p_j^{\alpha_j}}a_j)^k+n(\frac{q}{p_j^{\alpha_j}}a_j)}{q})\right|$$

Proof. Let $a=\sum_{j=1}^{t}\frac{q}{p_j^{\alpha_j}}a_j$, if a_j run through a reduced residue system modulo $p_j^{\alpha_j}$ $(j=1,2,\cdots,t)$, then a run through a reduced residue system modulo q . Note that

$$e(\frac{ma^k+na}{q})=e(\frac{m(\sum_{j=1}^{t}\frac{q}{p_j^{\alpha_j}}a_j)^k+n(\sum_{j=1}^{t}\frac{q}{p_j^{\alpha_j}}a_j)}{q})$$
$$=\prod_{j=1}^{t}e(\frac{m(\frac{q}{p_j^{\alpha_j}}a_j)^k+n(\frac{q}{p_j^{\alpha_j}}a_j)}{q}),$$

$$\chi(a)=\chi(\sum_{j=1}^{t}\frac{q}{p_j^{\alpha_j}}a_j)=\prod_{j=1}^{t}\chi_j(\frac{q}{p_j^{\alpha_j}}a_j)$$

so we have

$$\left|\sum_{a=1}^{q}{}'\chi(a)e(\frac{ma^k+na}{q})\right|=\left|\prod_{j=1}^{t}\sum_{a_j=1}^{p_j^{\alpha_j}}{}'\chi_j(\frac{q}{p_j^{\alpha_j}}a_j)e(\frac{m(\frac{q}{p_j^{\alpha_j}}a_j)^k+n(\frac{q}{p_j^{\alpha_j}}a_j)}{q})\right|$$
$$=\prod_{j=1}^{t}\left|\sum_{a_j=1}^{p_j^{\alpha_j}}{}'\chi_j(\frac{q}{p_j^{\alpha_j}}a_j)e(\frac{m(\frac{q}{p_j^{\alpha_j}}a_j)^k+n(\frac{q}{p_j^{\alpha_j}}a_j)}{q})\right|$$

This proves lemma 2.

Proof of the theorem and its generalization

By using lemma 1,2 in the above section, we now prove the theorem and its generalization.

Proof . From the properties of reduced systems, we have

$$\sum_{m=1}^{p}\sum_{\chi \bmod p}|c(m,n,k,\chi;p)|^4$$
$$=\sum_{m=1}^{p}\sum_{\chi \bmod p}|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi(a\overline{b})e(\frac{m(a^k-b^k)+n(a-b)}{p})|^2$$
$$=\sum_{m=1}^{p}\sum_{\chi \bmod p}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1}\chi(a\overline{c})e(\frac{m[b^k(a^k-1)-d^k(c^k-1)]+n[b(a-1)-d(c-1)]}{p})$$

From the orthogonality relation for Dirichlet character χ mod p^{α} ,we have

$$\sum_{m=1}^{p}\sum_{\chi \bmod p}|c(m,n,k,\chi;p)|^4$$
$$=\varphi(p)\sum_{m=1}^{p}\sum_{a=1}^{p-1}|\sum_{b=1}^{p-1}e(\frac{mb^k(a^k-1)+nb(a-1)}{p})|^2$$
$$=\begin{cases}(p-1)^3p+(p-1)\sum_{a=2}^{p-1}\sum_{m=1}^{p}|\sum_{b=1}^{p-1}e\left(\frac{m(a^k-1)b^k+n(a-1)b}{p}\right)|^2,(k,p-1)=1\\ (p-1)^3p+(p-1)p|\sum_{b=1}^{p-1}e(\frac{nb(p-2)}{p})|^2+(p-1)\sum_{a=2}^{p-2}\sum_{m=1}^{p}|\sum_{b=1}^{p-1}e\left(\frac{m(a^k-1)b^k+n(a-1)b}{p}\right)|^2,k=2\end{cases}$$

Note that if $(k, p-1)=1$, then

$$a^k - 1 \equiv 0(\bmod p) \Leftrightarrow a-1 \equiv 0(\bmod p).$$

if $(k, p-1)=1$， let r be arbitrary integer with $(r, p)=1$, then

$$(p-1)\sum_{m=1}^{p}\sum_{a=2}^{p-1}|\sum_{b=1}^{p-1}e(\frac{mb^k(a^k-1)+nb(a-1)}{p})|^2$$

$$=(p-1)\frac{1}{p-1}\sum_{r=1}^{p-1}\ \sum_{m=1}^{p}\sum_{a=2}^{p-1}|\sum_{b=1}^{p-1}e(\frac{m\bar{r}^k(rb)^k(a^k-1)+n(rb)(a-1)}{p})|^2$$

$$=\sum_{r=1}^{p}\ \sum_{m=1}^{p}\sum_{a=2}^{p-1}|\sum_{b=1}^{p-1}e(\frac{mb^k(a^k-1)+n(rb)(a-1)}{p})|^2$$

$$-\sum_{m=1}^{p}\sum_{a=2}^{p-1}|\sum_{b=1}^{p-1}e(\frac{mb^k(a^k-1)}{p})|^2$$

$$=\sum_{r=1}^{p}\ \sum_{m=1}^{p}\sum_{a=2}^{p-1}|\sum_{b=1}^{p-1}e(\frac{mb^k+nrb}{p})|^2-\sum_{m=1}^{p}\sum_{a=2}^{p-1}|\sum_{b=1}^{p-1}e(\frac{mb^k}{p})|^2$$

$$=(p-1)\sum_{m=1}^{p}\sum_{a=2}^{p-1}|\sum_{b=1}^{p-1}e(\frac{mb^k+nb}{p})|^2$$

Similarly, if $k=2$, then

$$(p-1)\sum_{m=1}^{p}\sum_{a=2}^{p-2}|\sum_{b=1}^{p-1}e(\frac{mb^k(a^k-1)+nb(a-1)}{p})|^2$$

$$=(p-1)\sum_{m=1}^{p}\sum_{a=2}^{p-2}|\sum_{b=1}^{p-1}e(\frac{mb^k+nb}{p})|^2$$

From lemma 1, the theorem could be obtained immediately.

$$\sum_{m=1}^{q}\sum_{\chi \bmod q}|c(m,n,k,\chi;q)|^4$$

$$=\prod_{j=1}^{t}(\sum_{\chi_j \bmod p_j}\sum_{m_j=1}^{p_j}\left|\sum_{a=1}^{p_j}{}'\chi_j(\frac{q}{p_j}a)e(\frac{(\frac{q}{p_j}m_j)(\frac{q}{p_j}a)^k+n(\frac{q}{p_j}a)}{q})\right|^4)$$

$$=\prod_{j=1}^{t}(\sum_{\chi_j \bmod p_j}\sum_{m_j=1}^{p_j}\left|\sum_{a=1}^{p_j}{}'\chi_j(a)e(\frac{m_ja^k+na}{p_j})\right|^4)$$

$$=\begin{cases}\prod_{j=1}^{t}(p_j-1)^2p_j(2p_j-3) & (k,p_j)=1\\ \prod_{j=1}^{t}(p_j-1)p_j(2p_j{}^2-7p_j+8) & k=2\end{cases}$$

$$=\begin{cases}q\varphi^2(q)\prod_{p\|q}(2p-3) & (k,\varphi(q))=1\\ q\varphi^2(q)\prod_{p\|q}(2p^2-7p+8) & k=2\end{cases}$$

This completes the proof of the generalization of theorem.

Acknowledgments

This work was supported in part by NSF grants of Hubei province Nos. 2011CDB081.

REFERENCES

[1] H.Darvenport, H.Heibronn.On an exponential sum. Proc.London Math. Soc. 41(1936) 449-453.

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

[3] Xu Zhefeng,Zhang Tianping,Zhang Wenpeng. On the mean value of the two-term exponential sums with Dirichlet characters. J. Number Theory 123(2)(2007) 352-362.

[4] C.CALDERON,M.J.DE VELASCO,M.J.ZARATE. An explicit formula for the fourth moment of certain exponential sums. Acta math.Hungar.130 (3)(2011) 203-222.

[5] L.K.Hua. Introduce to number theory. Science Press，Beijing，China，1979.

***Authors**: Doctor Aihua Luo (corresponding author), School of Mathematics and Statistics, South-Central University for Nationalities, Wuhan,China, E-mail: 7308627@qq.com;Doctor Hua Chen, School of science, Hubei University of Technology ,Hubei Wuhan,China, E-mail:249312654@qq.com.*