Journal of Inequalities and Applications
a SpringerOpen Journal

REVIEW Open Access

Some estimate of character sums and its applications

Jianghua Li[1] and Di Han[2*]

[*]Correspondence:
handi515@163.com
[2]Department of Mathematics, Northwest University, Xi'an, Shaanxi, P.R. China
Full list of author information is available at the end of the article

Abstract

The main purpose of this paper is using the elementary methods and the properties of Gauss sums to give a sharp estimate for some character sums. Then using this estimate to prove the existence of some special primitive roots mod p, an odd prime, and to prove that for any integer n with $(n,p)=1$, if p is large enough, then there exist two primitive roots $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ of p such that both $\boldsymbol{\alpha}+n\boldsymbol{\beta}$ and $n\bar{\boldsymbol{\alpha}}+\bar{\boldsymbol{\beta}}$ are also primitive roots of p, where $\bar{a}$ satisfies $\bar{a}a\equiv 1 \bmod p$. Let $N(n,p)$ denote the number of all pairs $(\boldsymbol{\alpha},\boldsymbol{\beta})$ of primitive roots of p such that both $\boldsymbol{\alpha}+n\boldsymbol{\beta}$ and $n\bar{\boldsymbol{\alpha}}+\bar{\boldsymbol{\beta}}$ are also primitive roots of p. Then we can give an interesting asymptotic formula for $N(n,p)$.

MSC: Primary 11M20

Keywords: primitive root of p; elementary method; estimate for character sums; asymptotic formula

1 Introduction

Let $q>1$ be an integer. For any integer n with $(n,q)=1$, from the well-known Euler-Fermat theorem, we have $n^{\phi(q)}\equiv 1 \bmod q$, where $\phi(q)$ is Euler ϕ-function. That is, $\phi(q)$ denotes the number of all integers $1\le a\le q$ with $(a,q)=1$. Let k be the smallest positive integer such that $n^k\equiv 1 \bmod q$. If $k=\phi(q)$, then n is called a primitive root of q. If q has a primitive root, then each reduced residue system mod q can be expressed as a geometric progression. This gives a powerful tool that can be used in problems involving reduced residue systems. Unfortunately, not all modulo q have primitive roots. In fact primitive roots exist only for the following several cases:

$$q=1,2,4,p^{\alpha},2p^{\alpha},$$

where p is an odd prime and $\alpha\ge 1$.

Many people have studied the properties of primitive roots and related problems, and obtained many interesting results; see [1–6] and [7]. For example, Juping Wang [4] proved that Golomb's conjecture is true for almost all $q=p^n$. That is, there exist two primitive elements α and β in finite fields $\mathbf{F}_q$ such that $\alpha+\beta=1$. Cohen and Mullen [2] established a generalization of Golomb's conjecture by proving the existence of $q_0>0$ such that, whenever $q>q_0$, there exist $\alpha,\beta\in\mathbf{F}_q$ with $\gamma\alpha+\delta\beta=\varepsilon$, where γ, δ and ε are arbitrary non-zero elements of $\mathbf{F}_q$.

In this paper, we consider the existence of some special primitive roots of p, such as all α, β, $\alpha+\beta$ and $\bar{\alpha}+\bar{\beta}$ are primitive roots of p, where $\bar{a}$ satisfies $\bar{a}a\equiv 1 \bmod p$. Furthermore,

© 2013 Li and Han; licensee Springer. This is an Open Access article distributed under the terms of the Creative Commons Attribution License (http://creativecommons.org/licenses/by/2.0), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

for any integer n with $(n,p) = 1$, are there primitive roots α and β of p such that both $\alpha + n\beta$ and $n\bar{\alpha} + \bar{\beta}$ are also two primitive roots of p? Let $N(n,p)$ denote the number of all pairs (α,β) of primitive roots of p such that both $\alpha + n\beta$ and $n\bar{\alpha} + \bar{\beta}$ are also primitive roots of p. How about the asymptotic properties of $N(n,p)$?

In this paper, we shall use the elementary methods and estimate for character sums to study this problem, and prove the following conclusion.

Theorem *Let p be an odd prime, then for any integer n with $(n,p) = 1$, we have the asymptotic formula*

$$N(n,p) = \frac{\phi^3(p-1)}{p-1}\prod_{q|p-1}\left(1 - \frac{1}{q-1} + \frac{1}{(q-1)^2}\right) + \theta \cdot \frac{\phi^4(p-1)}{(p-1)^4} \cdot p^{\frac{3}{2}} \cdot 16^{\omega(p-1)},$$

where $|\theta| \leq 5$, $\omega(m)$ denotes the number of all distinct prime divisors of m, $\prod_{q|p-1}$ denotes the product over all distinct prime divisors of $p-1$.

Taking $n = \pm 1$, from our theorem we may immediately deduce the following two corollaries.

Corollary 1 *Let p be a prime large enough, then there exist two primitive roots α and β of p such that both $\alpha + \beta$ and $\bar{\alpha} + \bar{\beta}$ are also primitive roots of p.*

Corollary 2 *Let p be a prime large enough, then there exist two primitive roots α and β of p such that both $\alpha - \beta$ and $\bar{\beta} - \bar{\alpha}$ are also primitive roots of p.*

2 Several lemmas

In this section, we shall give several lemmas, which are necessary in the proof of our theorem. Dirichlet characters and Gauss sums are used in this paper, please refer to [8] for more details. First we have the following lemma.

Lemma 1 *Let p be an odd prime, and let χ_1 and χ_2 be* mod p (*not all principal characters*). *Then, for any m with $(m,p) = 1$, we have the estimate*

$$\left|\sum_{a=1}^{p-1}\chi_1(a)\chi_2(ma+1)\right| \leq \sqrt{p}.$$

Proof If $\chi_1 = \chi_0$ is the principal character mod p, then we have

$$\begin{aligned}\sum_{a=1}^{p-1}\chi_1(a)\chi_2(ma+1) &= \sum_{a=1}^{p-1}\chi_2(ma+1)\\ &= \sum_{a=0}^{p-1}\chi_2(ma+1) - 1 = \sum_{a=0}^{p-1}\chi_2(a) - 1 = -1. \qquad (2.1)\end{aligned}$$

If $\chi_2 = \chi_0$, then we have

$$\sum_{a=1}^{p-1}\chi_1(a)\chi_2(ma+1) = \sum_{a=1}^{p-1}\chi_1(a)\chi_0(ma+1) = \sum_{a=1}^{p-1}\chi_1(a) - \chi_1(-\bar{m}) = -\chi_1(-\bar{m}). \qquad (2.2)$$

If neither χ_1 nor χ_2 is the principal character mod p, then from the properties of Gauss sums we have

$$\begin{aligned}\sum_{a=1}^{p-1}\chi_1(a)\chi_2(ma+1) &= \frac{1}{\tau(\bar{\chi}_2)}\sum_{a=1}^{p-1}\chi_1(a)\sum_{b=1}^{p-1}\bar{\chi}_2(b)e\left(\frac{b(ma+1)}{p}\right)\\ &= \frac{1}{\tau(\bar{\chi}_2)}\sum_{b=1}^{p-1}\bar{\chi}_2(b)\sum_{a=1}^{p-1}\chi_1(a)e\left(\frac{mba+b}{p}\right)\\ &= \frac{1}{\tau(\bar{\chi}_2)}\sum_{b=1}^{p-1}\bar{\chi}_2(b)e\left(\frac{b}{p}\right)\bar{\chi}_1(mb)\tau(\chi_1)\\ &= \bar{\chi}_1(m)\frac{\tau(\chi_1)}{\tau(\bar{\chi}_2)}\tau(\bar{\chi}_1\bar{\chi}_2).\end{aligned} \tag{2.3}$$

Note that both χ_1 and χ_2 are non-principal characters mod p, for any character χ mod$p$, $|\tau(\chi)| \le \sqrt{p}$ and $|\tau(\chi_1)| = |\tau(\chi_2)| = |\tau(\bar{\chi}_2)| = \sqrt{p}$. So from (2.3) we may immediately deduce the inequality

$$\left|\sum_{a=1}^{p-1}\chi_1(a)\chi_2(ma+1)\right| \le \sqrt{p}. \tag{2.4}$$

Now Lemma 1 follows from identities (2.1), (2.2) and estimate (2.4). □

Lemma 2 *Let p be an odd prime, and let* χ_1, χ_2, χ_3 *and* χ_4 *be four non-principal characters* mod p *with* $\chi_3\chi_4 \neq \chi_0$ (*or* $\chi_1 \neq \chi_4$). *Then, for any integer n with* $(n,p) = 1$, *we have the estimate*

$$\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_1(a)\chi_2(b)\chi_3(a+nb)\chi_4(n\bar{a}+\bar{b})\right| \le p^{\frac{3}{2}}.$$

Proof From the properties of reduced residue system mod p, we have

$$\begin{aligned}&\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_1(a)\chi_2(b)\chi_3(a+nb)\chi_4(n\bar{a}+\bar{b})\\ &\quad= \sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_1(ab)\chi_2(b)\chi_3(ab+nb)\chi_4(n\bar{a}\bar{b}+\bar{b})\\ &\quad= \sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_1\chi_2\chi_3\bar{\chi}_4(b)\chi_1\bar{\chi}_4(a)\chi_3\chi_4(a+n).\end{aligned} \tag{2.5}$$

It is clear that for any character χ mod p, we have

$$\sum_{a=1}^{p-1}\chi(a) = \begin{cases} p-1 & \text{if } \chi \text{ is the principal character mod } p,\\ 0 & \text{otherwise.}\end{cases} \tag{2.6}$$

So, if $\chi_1\chi_2\chi_3\bar{\chi}_4 \neq \chi_0$, the principal character mod p, then from (2.5) and (2.6) we have the identity

$$\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_1(a)\chi_2(b)\chi_3(a+nb)\chi_4(n\bar{a}+\bar{b})\right| = 0. \tag{2.7}$$

If $\chi_1\chi_2\chi_3\bar{\chi}_4 = \chi_0$, note that $\chi_1\bar{\chi}_4$ and $\chi_3\chi_4$ not all principal characters mod p, so from (2.5), (2.6) and Lemma 1 we have the estimate

$$\begin{aligned}
&\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_1(a)\chi_2(b)\chi_3(a+nb)\chi_4(n\bar{a}+\bar{b})\right| \\
&\quad= \left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_1\chi_2\chi_3\bar{\chi}_4(b)\chi_1\bar{\chi}_4(a)\chi_3\chi_4(a+n)\right| \\
&\quad= (p-1)\cdot\left|\sum_{a=1}^{p-1}\chi_1\bar{\chi}_4(a)\chi_3\chi_4(a+n)\right| \le p^{\frac{3}{2}}.
\end{aligned} \tag{2.8}$$

Combining (2.7) and (2.8), we may immediately deduce Lemma 2. □

Lemma 3 *Let p be an odd prime. Then, for any integer c with* $(c,p)=1$, *we have the identity*

$$\frac{\phi(p-1)}{p-1}\sum_{h|p-1}\frac{\mu(h)}{\phi(h)}\sum_{\substack{k=1\\(h,k)=1}}^{h} e\left(\frac{k\operatorname{ind}c}{h}\right) = \begin{cases}1 & \textit{if } c \textit{ is a primitive root of } p,\\ 0 & \textit{otherwise,}\end{cases}$$

where $\operatorname{ind}c$ *denotes the index of c relative to some fixed primitive root of p,* $\mu(n)$ *is the Möbius function.*

Proof See Proposition 2.2 of reference [9]. □

3 Proof of the theorem

In this section, we shall complete the proof of our theorem. First we write $\chi_{s,h}(c) = e(\frac{s\operatorname{ind}c}{h})$. It is clear that $\chi_{s,h}(c)$ is a Dirichlet character mod p. For any integer n with $(n,p)=1$, from Lemma 3 we have

$$\begin{aligned}
&N(n,p) \\
&\quad= \sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\frac{\phi^4(p-1)}{(p-1)^4}\sum_{h|p-1}\sum_{i|p-1}\sum_{j|p-1}\sum_{k|p-1}\frac{\mu(h)}{\phi(h)}\frac{\mu(i)}{\phi(i)}\frac{\mu(j)}{\phi(j)}\frac{\mu(k)}{\phi(k)} \\
&\quad\quad\times\sum_{\substack{h_1=1\\(h,h_1)=1}}^{h}\sum_{\substack{i_1=1\\(i,i_1)=1}}^{i}\sum_{\substack{j_1=1\\(j,j_1)=1}}^{j}\sum_{\substack{k_1=1\\(k,k_1)=1}}^{k}\chi_{h_1,h}(a)\chi_{i_1,i}(b)\chi_{j_1,j}(a+nb)\chi_{k_1,k}(n\bar{a}+\bar{b}) \\
&\quad= \frac{\phi^4(p-1)}{(p-1)^2} + 2\frac{\phi^4(p-1)}{(p-1)^3}\sum_{\substack{h|p-1\\h>1}}\frac{\mu(h)}{\phi(h)}\sum_{\substack{s=1\\(h,s)=1}}^{h}\sum_{a=1}^{p-1}\chi_{s,h}(a)
\end{aligned}$$

$$+ 2\frac{\phi^4(p-1)}{(p-1)^4}\sum_{\substack{u|p-1\\u>1}}\frac{\mu(u)}{\phi(u)}\sum_{\substack{v=1\\(v,u)=1}}^{u}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_{v,u}(a+nb)$$

$$+ \frac{\phi^4(p-1)}{(p-1)^4}\sum_{\substack{h|p-1\\h>1}}\sum_{\substack{u|p-1\\u>1}}\frac{\mu(h)}{\phi(h)}\frac{\mu(u)}{\phi(u)}\sum_{\substack{s=1\\(h,s)=1}}^{h}\sum_{\substack{v=1\\(v,u)=1}}^{u}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_{v,u}(a)\chi_{s,h}(b)$$

$$+ \frac{\phi^4(p-1)}{(p-1)^4}\sum_{\substack{h|p-1\\h>1}}\sum_{\substack{u|p-1\\u>1}}\frac{\mu(h)}{\phi(h)}\frac{\mu(u)}{\phi(u)}\sum_{\substack{s=1\\(h,s)=1}}^{h}\sum_{\substack{v=1\\(v,u)=1}}^{u}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_{v,u}(a+nb)\chi_{s,h}(n\bar{a}+\bar{b})$$

$$+ \frac{\phi^4(p-1)}{(p-1)^4}\sum_{\substack{h|p-1\\h>1}}\sum_{\substack{u|p-1\\u>1}}\frac{\mu(h)}{\phi(h)}\frac{\mu(u)}{\phi(u)}\sum_{\substack{s=1\\(h,s)=1}}^{h}\sum_{\substack{v=1\\(v,u)=1}}^{u}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_{v,u}(a)\chi_{s,h}(n\bar{a}+\bar{b})$$

$$+ \frac{\phi^4(p-1)}{(p-1)^4}\sum_{\substack{h|p-1\\h>1}}\sum_{\substack{u|p-1\\u>1}}\frac{\mu(h)}{\phi(h)}\frac{\mu(u)}{\phi(u)}\sum_{\substack{s=1\\(h,s)=1}}^{h}\sum_{\substack{v=1\\(v,u)=1}}^{u}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_{v,u}(b)\chi_{s,h}(n\bar{a}+\bar{b})$$

$$+ \frac{\phi^4(p-1)}{(p-1)^4}\sum_{\substack{h|p-1\\h>1}}\sum_{\substack{u|p-1\\u>1}}\frac{\mu(h)}{\phi(h)}\frac{\mu(u)}{\phi(u)}\sum_{\substack{s=1\\(h,s)=1}}^{h}\sum_{\substack{v=1\\(v,u)=1}}^{u}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_{s,h}(a)\chi_{v,u}(a+nb)$$

$$+ \frac{\phi^4(p-1)}{(p-1)^4}\sum_{\substack{h|p-1\\h>1}}\sum_{\substack{u|p-1\\u>1}}\frac{\mu(h)}{\phi(h)}\frac{\mu(u)}{\phi(u)}\sum_{\substack{s=1\\(h,s)=1}}^{h}\sum_{\substack{v=1\\(v,u)=1}}^{u}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_{s,h}(b)\chi_{v,u}(a+nb)$$

$$+ \frac{\phi^4(p-1)}{(p-1)^4}\sum_{\substack{i|p-1\\i>1}}\sum_{\substack{j|p-1\\j>1}}\sum_{\substack{k|p-1\\k>1}}\frac{\mu(i)}{\phi(i)}\frac{\mu(j)}{\phi(j)}\frac{\mu(k)}{\phi(k)}$$

$$\times \sum_{\substack{i_1=1\\(i,i_1)=1}}^{i}\sum_{\substack{j_1=1\\(j,j_1)=1}}^{j}\sum_{\substack{k_1=1\\(k,k_1)=1}}^{k}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_{i_1,i}(b)\chi_{j_1,j}(a+nb)\chi_{k_1,k}(n\bar{a}+\bar{b})$$

$$+ \frac{\phi^4(p-1)}{(p-1)^4}\sum_{\substack{h|p-1\\h>1}}\sum_{\substack{j|p-1\\j>1}}\sum_{\substack{k|p-1\\k>1}}\frac{\mu(h)}{\phi(h)}\frac{\mu(j)}{\phi(j)}\frac{\mu(k)}{\phi(k)}$$

$$\times \sum_{\substack{h_1=1\\(h,h_1)=1}}^{h}\sum_{\substack{j_1=1\\(j,j_1)=1}}^{j}\sum_{\substack{k_1=1\\(k,k_1)=1}}^{k}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_{h_1,h}(a)\chi_{j_1,j}(a+nb)\chi_{k_1,k}(n\bar{a}+\bar{b})$$

$$+ \frac{\phi^4(p-1)}{(p-1)^4}\sum_{\substack{h|p-1\\h>1}}\sum_{\substack{i|p-1\\i>1}}\sum_{\substack{k|p-1\\k>1}}\frac{\mu(h)}{\phi(h)}\frac{\mu(i)}{\phi(i)}\frac{\mu(k)}{\phi(k)}$$

$$\times \sum_{\substack{h_1=1\\(h,h_1)=1}}^{h}\sum_{\substack{i_1=1\\(i,i_1)=1}}^{i}\sum_{\substack{k_1=1\\(k,k_1)=1}}^{k}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_{h_1,h}(a)\chi_{i_1,i}(b)\chi_{k_1,k}(n\bar{a}+\bar{b})$$

$$+ \frac{\phi^4(p-1)}{(p-1)^4}\sum_{\substack{h|p-1\\h>1}}\sum_{\substack{i|p-1\\i>1}}\sum_{\substack{j|p-1\\j>1}}\frac{\mu(h)}{\phi(h)}\frac{\mu(i)}{\phi(i)}\frac{\mu(j)}{\phi(j)}$$

$$\times \sum_{\substack{h_1=1\\(h,h_1)=1}}^{h} \sum_{\substack{i_1=1\\(i,i_1)=1}}^{i} \sum_{\substack{j_1=1\\(j,j_1)=1}}^{j} \sum_{a=1}^{p-1}\sum_{b=1}^{p-1} \chi_{h_1,h}(a)\chi_{i_1,i}(b)\chi_{j_1,j}(a+nb)$$

$$+ \frac{\phi^4(p-1)}{(p-1)^4} \sum_{\substack{h|p-1\\h>1}}\sum_{\substack{i|p-1\\i>1}}\sum_{\substack{j|p-1\\j>1}}\sum_{\substack{k|p-1\\k>1}} \frac{\mu(h)}{\phi(h)}\frac{\mu(i)}{\phi(i)}\frac{\mu(j)}{\phi(j)}\frac{\mu(k)}{\phi(k)}$$

$$\times \sum_{\substack{h_1=1\\(h,h_1)=1}}^{h} \sum_{\substack{i_1=1\\(i,i_1)=1}}^{i} \sum_{\substack{j_1=1\\(j,j_1)=1}}^{j} \sum_{\substack{k_1=1\\(k,k_1)=1}}^{k} \sum_{a=1}^{p-1}\sum_{b=1}^{p-1} \chi_{h_1,h}(a)\chi_{i_1,i}(b)\chi_{j_1,j}(a+nb)\chi_{k_1,k}(n\bar{a}+\bar{b}). \tag{3.1}$$

Now we estimate each term in (3.1) respectively. It is clear that for any integer $h > 1$ and $(s,h) = 1$, we have the identity

$$\sum_{a=1}^{p-1} \chi_{s,h}(a) = 0. \tag{3.2}$$

For any three non-principal characters χ_1, χ_2 and χ_3 mod p, from Lemma 2 we have

$$\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1} \chi_1(a)\chi_2(b)\chi_3(a+nb)\right| = \left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1} \chi_1\chi_2\chi_3(b)\chi_1(a)\chi_3(a+n)\right| \le p^{\frac{3}{2}}, \tag{3.3}$$

$$\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1} \chi_1(a)\chi_2(b)\chi_3(n\bar{a}+\bar{b})\right| \le p^{\frac{3}{2}}, \tag{3.4}$$

$$\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1} \chi_1(a)\chi_2(a+nb)\chi_3(n\bar{a}+\bar{b})\right| \le p^{\frac{3}{2}}, \tag{3.5}$$

$$\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1} \chi_1(b)\chi_2(a+nb)\chi_3(n\bar{a}+\bar{b})\right| \le p^{\frac{3}{2}}. \tag{3.6}$$

From Lemma 1 we know that for any two non-principal characters χ_1 and χ_2 mod p, we have the estimates

$$\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1} \chi_1(a)\chi_2(a+nb)\right| \le p^{\frac{3}{2}}, \tag{3.7}$$

$$\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1} \chi_1(b)\chi_2(a+nb)\right| \le p^{\frac{3}{2}}, \tag{3.8}$$

$$\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1} \chi_1(a)\chi_2(n\bar{a}+\bar{b})\right| \le p^{\frac{3}{2}}, \tag{3.9}$$

$$\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1} \chi_1(b)\chi_2(n\bar{a}+\bar{b})\right| \le p^{\frac{3}{2}}, \tag{3.10}$$

$$\left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1} \chi_1(a+nb)\chi_2(n\bar{a}+\bar{b})\right| = \left|\sum_{a=1}^{p-1}\sum_{b=1}^{p-1} \chi_1(b)\bar{\chi}_2(b)\bar{\chi}_1(a)\chi_1\chi_2(a+n)\right| \le p^{\frac{3}{2}}. \tag{3.11}$$

If four characters $\chi_{h_1,h}$, $\chi_{i_1,i}$, $\chi_{j_1,j}$ and $\chi_{k_1,k}$ in the last term of (3.1) do not satisfy the condition of Lemma 2, this time from Lemma 2 and the orthogonality of characters mod p we have

$$\begin{aligned}
&\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_{h_1,h}(a)\chi_{i_1,i}(b)\chi_{j_1,j}(a+nb)\chi_{k_1,k}(n\bar{a}+\bar{b}) \\
&\quad=\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_{h_1,h}\chi_{i_1,i}\chi_{j_1,j}\bar{\chi}_{k_1,k}(b)\chi_{h_1,h}\bar{\chi}_{k_1,k}(a)\chi_{j_1,j}\chi_{k_1,k}(a+n) \\
&\quad=\begin{cases}(p-1)\sum_{a=1}^{p-1}\chi_{h_1,h}\bar{\chi}_{k_1,k}(a)\chi_{j_1,j}\chi_{k_1,k}(a+n) & \text{if } \chi_{h_1,h}\chi_{i_1,i}\chi_{j_1,j}\bar{\chi}_{k_1,k}=\chi_0; \\ 0 & \text{if } \chi_{h_1,h}\chi_{i_1,i}\chi_{j_1,j}\bar{\chi}_{k_1,k}\neq\chi_0,\end{cases} \\
&\quad=\begin{cases}\leq p^{\frac{3}{2}} & \text{if } \chi_{i_1,i}\chi_{j_1,j}\neq\chi_0 \text{ or } \chi_{h_1,h}\neq\chi_{k_1,k}; \\ (p-1)\cdot\sum_{a=1}^{p-1}\chi_0(a+n) & \text{if } \chi_{h_1,h}=\chi_{i_1,i}=\chi_{k_1,k} \text{ and } \chi_{j_1,j}=\bar{\chi}_{k_1,k}; \\ 0 & \text{if } \chi_{h_1,h}\chi_{i_1,i}\chi_{j_1,j}\bar{\chi}_{k_1,k}\neq\chi_0.\end{cases} \qquad (3.12)
\end{aligned}$$

Note that the identity $\sum_{h|p-1}|\mu(h)|=2^{\omega(p-1)}$, $\chi_{h_1,h}=\chi_{i_1,i}=\chi_{k_1,k}$ and $\chi_{i_1,i}=\bar{\chi}_{j_1,j}$ implies $h=i=j=k$, $h_1=i_1=k_1$ and $j_1=k-h_1$. So from (3.1)-(3.12) we have

$$\begin{aligned}
N(n,p)&=\frac{\phi^4(p-1)}{(p-1)^2}+R_1\cdot\frac{\phi^4(p-1)}{(p-1)^4}\cdot p^{\frac{3}{2}}\cdot 16^{\omega(p-1)} \\
&\quad+\frac{\phi^4(p-1)}{(p-1)^4}\sum_{\substack{h|p-1\\h>1}}\frac{|\mu(h)|^4}{\phi^4(h)}\sum_{\substack{s=1\\(s,h)=1)}}^{h}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_0(a+n) \\
&=\frac{\phi^3(p-1)}{p-1}\prod_{q|p-1}\left(1-\frac{1}{q-1}+\frac{1}{(q-1)^2}\right)+R\cdot\frac{\phi^4(p-1)}{(p-1)^4}\cdot p^{\frac{3}{2}}\cdot 16^{\omega(p-1)},
\end{aligned}$$

where we have used the identity $\sum_{h|p-1}\frac{|\mu(h)|^4}{\phi^3(h)}=\frac{p-1}{\phi(p-1)}\prod_{q|p-1}(1-\frac{1}{q-1}+\frac{1}{(q-1)^2})$, and $|R|\leq 5$. This completes the proof of our theorem.

Competing interests

The authors declare that they have no competing interests.

Authors' contributions

JL carried out the sharp estimate for some character sums and give an asymptotic formula for $N(n,p)$. DH participated in the research and summary of the study.

Author details

[1]College of Science, Xi'an University of Technology, Xi'an, Shaanxi, P.R. China. [2]Department of Mathematics, Northwest University, Xi'an, Shaanxi, P.R. China.

Acknowledgements

The authors would like to thank the referee for carefully examining this paper and providing a number of important comments. This work is supported by the N.S.F. (11071194, 61202437) of P.R. China, N.S.F. of Shaanxi Province (2012K06-43) and Foundation of Shaanxi Educational Committee (12JK0874).

Received: 12 April 2013 Accepted: 4 July 2013 Published: 18 July 2013

References

1. Cohen, SD, Zhang, W: Sums of two exact powers. Finite Fields Appl. **8**, 471-477 (2002)
2. Cohen, SD, Mullen, GL: Primitive elements in Costas arrays. Appl. Algebra Eng. Commun. Comput. **2**, 45-53 (1991) (Corrections) **2**, 297-299 (1992)

3. Golomb, S: On the algebraic construction for Costas arrays. J. Comb. Theory, Ser. A **37**, 13-21 (1984)
4. Wang, J: On Golomb's conjecture. Sci. China Ser. A **9**, 927-935 (1987)
5. Wang, P, Cao, X, Feng, R: On the existence of some specific elements in finite fields of characteristic 2. Finite Fields Appl. **18**, 800-813 (2012)
6. Tian, T, Qi, W: Primitive normal element and its inverse in finite fields. Acta Math. Sin. **49**, 657-668 (2006)
7. Zhang, W: On a problem related to Golomb's conjecture. J. Syst. Sci. Complex. **16**, 13-18 (2003)
8. Apostol, TM: Introduction to Analytic Number Theory. Springer, New York (1976)
9. Narkiewicz, W: Classical Problems in Number Theory, pp. 79-80. PWN-Polish Scientific Publishers, Warszawa (1987)

doi:10.1186/1029-242X-2013-328
Cite this article as: Li and Han: **Some estimate of character sums and its applications.** *Journal of Inequalities and Applications* 2013 **2013**:328.

Submit your manuscript to a SpringerOpen journal and benefit from:

► Convenient online submission
► Rigorous peer review
► Immediate publication on acceptance
► Open access: articles freely available online
► High visibility within the field
► Retaining the copyright to your article

Submit your next manuscript at ► springeropen.com