ORIGINAL RESEARCH

Elements of $\mathbb{Z}_q^*$ represented as sum of two special elements

Zhefeng Xu[1] · Jiankang Wang[1]

Received: 1 June 2022 / Accepted: 12 September 2025 / Published online: 26 September 2025

Abstract
Let $q = p^\alpha$ for a prime $p \geq 3$ and a positive integer α, let $\mathbb{Z}_q^*$ be a reduced residue system modulo q, k be an integer with $k \mid \phi(q)$. The purpose of this paper is to give an asymptotic property for $N_k(n, q)$, the number of representations of any element $n \in \mathbb{Z}_q^*$ as sum of a primitive root and a k-th residue in $\mathbb{Z}_q^*$. In addition, we consider the square mean value of the error term of $N_2(n, p)$ in this short note.

Keywords Primitive root · k-th residue · Finite ring · Asymptotic formula

1 Introduction

Let $q = p^\alpha$ for a prime $p \geq 3$ and a positive integer α. We know that there are $\phi(\phi(q))$ primitive roots in $\mathbb{Z}_q^*$, where $\mathbb{Z}_q^*$ is the reduced residue system modulo q and $\phi(q)$ is the Euler function.

Let g be a primitive root modulo p. Andrew Odlyzko conjectured that one can take N to be as small as $p^{1/2+\epsilon}$, then every element $a \in \mathbb{Z}_p^*$ has at least one representation of the form

$$a \equiv g^x - g^y \pmod{p}, \quad 1 \leq x, y \leq N.$$

Rudnick and Zaharescu [10] proved that one can take $cp^{\frac{3}{4}} \ln p$ for some $c > 0$ by using standard methods of characters sums. On this basis, Garaev, Cilleruelo and other scholars also gave some results (for details see [1, 4, 5, 10]).

Denote by $\mathbb{F}_q$ the finite field of order q, Golomb [6] conjectured that there exists a constant $q_0 \geq 0$ such that every nonzero element $\varepsilon \in \mathbb{F}_q$ has at least one representation of the form $\varepsilon = \alpha + \beta$ for all $q \geq q_0$, where $\alpha, \beta \in \mathbb{F}_q$ are primitive roots (generators).

In 1991, Cohen and Mullen [2] established a generalization of Golomb's conjectures by proving the existence of $q_0 > 0$ such that, whenever $q > q_0$, there exist two primitive roots $\alpha, \beta \in \mathbb{F}_q$ with $\varepsilon = \gamma\alpha + \delta\beta$ for arbitrary nonzero elements $\gamma, \delta, \varepsilon \in \mathbb{F}_q$. For more general, Cohen and Zhang [3] investigated the problem: For given divisors k, l of $q - 1$, whether there exists a pair of primitive roots $\alpha, \beta \in \mathbb{F}_q$ such that

$$\varepsilon = \gamma\alpha^k + \delta\beta^l.$$

Communicated by B. Sury

This work is supported by National Natural Science Foundation of China (12471006, 12501009).

Denote by $N_{k,l}(q, \varepsilon, \gamma, \delta)$ the number of solutions of this equation and they obtained the following asymptotic formula

$$N_{k,l}(q, \varepsilon, \gamma, \delta) = \sigma^2(q-1)\left\{q - 1 + \theta klW\left(\frac{q-1}{k}\right)W\left(\frac{q-1}{l}\right)\sqrt{q}\right\},$$

where $\sigma(m) = \frac{\phi(m)}{m}$, $|\theta| \leq 1$ and $W(m) = 2^{\omega(m)}$, $\omega(m)$ denotes the number of distinct prime factors of m.

On the other hand, Zhang [12] studied that for each element $a \in \mathbb{F}_q$ whether there exists a pair of primitive roots $g_1, g_2 \in \mathbb{F}_q$ such that

$$a^2 = g_1 g_2,$$

and obtained that every square element of $\mathbb{F}_q$ can be represented as a product of two primitive elements:

Proposition 1 *i) For any quadratic residue a in the finite field $\mathbb{F}_p$, there exist two primitive roots $g_1, g_2 \in \mathbb{F}_p$ such that*

$$a = g_1 g_2;$$

ii) For any quadratic non-residue a in the finite field $\mathbb{F}_p$, there exist three primitive roots $g_1, g_2, g_3 \in \mathbb{F}_p$ such that

$$a = g_1 g_2 g_3.$$

These properties interpret the relationship between quadratic residues and primitive roots in $\mathbb{F}_p$.

In this paper, we consider the representation of elements of $\mathbb{Z}_q^*$ as sum (or other form) of some special elements in $\mathbb{Z}_q^*$. And we give the following specific problem. For each element $n \in \mathbb{Z}_q^*$, whether there exists a primitive root g and a k-th residue s in $\mathbb{Z}_q^*$ such that

$$n = g + s. \tag{1}$$

Let $N_k(n, p)$ denote the number of solutions of (1), we have the following results

Theorem 1 *Let p be a prime ≥ 3, let $q = p^\alpha$ for a positive integer α and $k|\phi(q)$ for a positive integer k. Then for any element $n \in \mathbb{Z}_q^*$, there holds*

$$N_k(n, q) = \frac{\phi(\phi(q))\phi(q)}{kq} + \xi\frac{\phi(\phi(q))}{\phi(q)}2^{\omega(\phi(q))}qp^{-\frac{1}{2}},$$

where $|\xi| \leq 1$.

This theorem tell us a fact in $\mathbb{Z}_q^*$: if q satisfies $\frac{\phi(\phi(q))\phi(q)}{kq} > \frac{\phi(\phi(q))}{\phi(q)}2^{\omega(\phi(q))}qp^{-\frac{1}{2}}$, then any element in $\mathbb{Z}_q^*$ can be represented as sum of a primitive root and a k-th residue, and the number of representations is:

$$\frac{\phi(\phi(q))\phi(q)}{kq} + \xi\frac{\phi(\phi(q))}{\phi(q)}2^{\omega(\phi(q))}qp^{-\frac{1}{2}}.$$

Taking $k = 2$, we have the following result for quadratic residues:

Corollary 1 *Let $q = p^\alpha$ for a prime $p \geq 3$ and a positive integer α. For an arbitrary element $n \in \mathbb{Z}_q^*$, we have*

$$N_2(n, q) = \frac{\phi(\phi(q))\phi(q)}{2q} + \xi\frac{\phi(\phi(q))}{\phi(q)}2^{\omega(\phi(q))}qp^{-\frac{1}{2}}.$$

At this point, note that

$$\omega(n) \le c\frac{\ln n}{\ln\ln n},$$

where $c = 1.38402...$, then we have

$$2^{\omega(n)} \le 2^{c\frac{\ln n}{\ln\ln n}} < n^{\frac{c\ln 2}{\ln\ln n}}.$$

It is obvious that if $e^e \le m \le n$ then

$$m^{\frac{c\ln 2}{\ln\ln m}} \le n^{\frac{c\ln 2}{\ln\ln n}}.$$

According to $\frac{\phi^2(q)}{q} > 2q^{1+\frac{c\ln 2}{\ln\ln q}}p^{-\frac{1}{2}}$, it follows that $q > e^{e^{2\alpha}+e}$. Thus, if $q > e^{e^{2\alpha}+e}$ then there exists a primitive root g and a k-th residue s such that $n = g + s$ in $\mathbb{Z}_q^*$ for any element $n \in \mathbb{Z}_q^*$. In addition, we can calculate the existence of g and s one by one for $q < e^{e^{2\alpha}+e}$ by using computer.

If $q = p$ is prime, then we have $e^{e^2+e} < 2.46 \times 10^4$. We calculate this one by one for all odd primes $p < 2.46 \times 10^4$ by using computer and obtain that arbitrary nonzero elements of $\mathbb{F}_p$ can be represented as sum of a primitive root and a quadratic residue in $\mathbb{F}_p$ for all odd primes except 3,7. If $q = p^2$, then $e^{e^4+e} > 5 \times 10^{24}$. It is difficult to calculate this for all odd primes $p < 5 \times 10^{24}$.

Similarly, we can know that whether arbitrary elements of $\mathbb{Z}_q^*$ are represented as the sum of a primitive root and a k-th residue in $\mathbb{Z}_q^*$ for all $q = p^\alpha$ and a given $k|\phi(q)$.

Combining Proposition 2, we also have

Corollary 2 *Let p be an odd prime except 3,7. For any nonzero element $\varepsilon \in \mathbb{F}_p$, there exist three primitive roots $g_1, g_2, g_3 \in \mathbb{F}_p$ such that*

$$\varepsilon = g_1 + g_2g_3.$$

Corollary 3 *Let p be a prime > 7. For any nonzero element $\varepsilon \in \mathbb{F}_p$, there exist four primitive roots $g_1, g_2, g_3, g_4 \in \mathbb{F}_p$ such that*

$$\varepsilon = g_1 + g_2g_3g_4.$$

Let $E_k(n,q) = N_k(n,q) - \frac{\phi(\phi(q))\phi(q)}{kq}$, we have

Theorem 2 *Let p be a prime ≥ 3. Then we have*

$$\sum_{n=1}^{p} E_2^2(n,p) = \frac{\phi(p-1)}{4}(p - \phi(p-1)) + \lambda 2^{2\omega(p-1)}p^{\frac{3}{2}},$$

where $|\lambda| \le 1$.

Remark The result of theorem 2 shows that the order of error term be close to the best in Theorem 1.

2 Proof of the theorems

To prove theorems, we need the following lemmas.

Lemma 1 *Let p be an odd prime and let α be a positive integer, n be an integer with $(n,p) = 1$. Then*

$$\sum_{d|\phi(p^\alpha)} \frac{\mu(d)}{\phi(d)} \sum_{\substack{h=1\\(h,d)=1}}^{d} e\left(\frac{h\ ind\ n}{d}\right) = \begin{cases} \frac{\phi(p^\alpha)}{\phi(\phi(p^\alpha))}, & \text{if } n \text{ is a primitive root modulo } p^\alpha; \\ 0, & \text{otherwise}, \end{cases}$$

where $ind\ n$ satisfies $n \equiv g^{ind\ n} \pmod p$ for a fixed primitive root g modulo p^α, $\mu(n)$ is the Möbius function.

Proof It is easy to show that

$$\sum_{\substack{h=1\\(h,d)=1}}^{d} e\left(\frac{h\ ind\ n}{d}\right)$$

is a multiplicative function of d, $\mu(d)$ and $\phi(d)$ are also multiplicative. Via properties of multiplicative function, we have

$$\sum_{d|\phi(p^\alpha)} \frac{\mu(d)}{\phi(d)} \sum_{\substack{h=1\\(h,d)=1}}^{d} e\left(\frac{h\ ind\ n}{d}\right) = \prod_{p_1|\phi(p^\alpha)} \left(1 + \frac{\mu(p_1)}{\phi(p_1)} \sum_{\substack{h=1\\(h,p_1)=1}}^{p_1} e\left(\frac{h\ ind\ n}{p_1}\right)\right),$$

where $\prod_{p_1|\phi(p^\alpha)}$ denotes the product of all different prime factors of $\phi(p^\alpha)$.

If n is not a primitive root modulo p^α, $(ind\ n, \phi(p^\alpha)) > 1$. Then, there has a prime factor p_1 of $\phi(p^\alpha)$ such that $p_1|ind\ n$, we have

$$1 + \frac{\mu(p_1)}{\phi(p_1)} \sum_{\substack{h=1\\(h,p_1)=1}}^{p_1} e\left(\frac{h\ ind\ n}{p_1}\right) = 1 + \frac{\mu(p_1)}{\phi(p_1)}\phi(p_1) = 0.$$

If n is a primitive root modulo p^α, then $(ind\ n, \phi(p^\alpha)) = 1$. Thus,

$$\prod_{p_1|\phi(p^\alpha)} \left(1 + \frac{\mu(p_1)}{\phi(p_1)} \sum_{\substack{h=1\\(h,p_1)=1}}^{p_1} e\left(\frac{h\ ind\ n}{p_1}\right)\right) = \prod_{p_1|\phi(p^\alpha)} \left(1 + \frac{\mu(p_1)}{\phi(p_1)}\mu(p_1)\right) = \frac{\phi(p^\alpha)}{\phi(\phi(p^\alpha))}.$$

This proves Lemma 1. □

Lemma 2 *Let p be an odd prime, α be a positive integer and let χ_1, χ_2 be any Dirichlet characters modulo p^α with not all principal. Define Jacobi sums by*

$$J(\lambda, \chi_1, \chi_2, p^\alpha) = \sum_{x=1}^{p^\alpha} \chi_1(x)\chi_2(\lambda - x).$$

Then for any $\lambda \in \mathbb{Z}^*_{p^\alpha}$, we have

$$|J(\lambda, \chi_1, \chi_2, p^\alpha)| \le p^{\alpha-\frac{1}{2}}.$$

Proof For any Dirichlet characters χ_1, χ_2 modulo p^α such that at least one of them is primitive, according to results in [7, 9, 11], we have

$$|J(\lambda, \chi_1, \chi_2, p^\alpha)| \le p^{\frac{\alpha}{2}}.$$

If χ_1, χ_2 both are not primitive, we know that if χ is not a primitive modulo p^α then χ is a Dirichlet character modulo $p^{\alpha-1}$, we can reduce to a lower modulus

$$J(\lambda, \chi_1, \chi_2, p^\alpha) = pJ(\xi, \chi_1, \chi_2, p^{\alpha-1}),$$

where $\xi \equiv \lambda \pmod{p^{\alpha-1}}$. From the properties of Dirichlet characters modulo p^α, let χ_1, χ_2 be the nonprimitive Dirichlet characters modulo p^β, $2 \le \beta \le \alpha$, then we have

$$|J(\lambda, \chi_1, \chi_2, p^\alpha)| = p^{\alpha-1}|J(\eta, \chi_1, \chi_2, p)| = p^{\alpha-\frac{1}{2}}, \tag{2}$$

where $\eta \equiv \lambda \pmod{p}$. This proves Lemma 2. □

Now we use the lemmas to prove theorems.

Proof of Theorem 1 Let $q = p^\alpha$. Denote by G the set of primitive roots in $\mathbb{Z}_q^*$ and let R_k be the set of k-th residues in $\mathbb{Z}_q^*$, we know that $k|\phi(q)$. Note that the trigonometric identity

$$\sum_{a=1}^{m} e\left(\frac{au}{m}\right) = \begin{cases} m & \text{if} m|u; \\ 0, & \text{if} m \nmid u, \end{cases} \tag{3}$$

and

$$|G| = \phi(\phi(q)),\ |R_k| = \frac{\phi(q)}{k}.$$

From the definition of $N_k(n, q)$, we have

$$\begin{aligned} N_k(n,q) = & \sum_{\substack{a=1 \\ a\in G}}^{q-1} \sum_{\substack{b=1 \\ b\in R_k}}^{q-1} 1 \\ & \quad a+b\equiv n(\bmod q) \\ =& \frac{1}{q}\sum_{c=1}^{q} e\left(\frac{-cn}{q}\right) \sum_{\substack{a=1 \\ a\in G}}^{q-1} e\left(\frac{ac}{q}\right) \sum_{\substack{b=1 \\ b\in R_k}}^{q-1} e\left(\frac{bc}{q}\right) \\ =& \frac{\phi(\phi(q))\phi(q)}{kq} + \frac{1}{q}\sum_{c=1}^{q-1} e\left(\frac{-cn}{q}\right) \sum_{\substack{a=1 \\ a\in G}}^{q-1} e\left(\frac{ac}{q}\right) \sum_{\substack{b=1 \\ b\in R_k}}^{q-1} e\left(\frac{bc}{q}\right) \\ =& \frac{\phi(\phi(q))\phi(q)}{kq} + E_k(n,q). \end{aligned} \tag{4}$$

According to Lemma 1, it follows that

$$\begin{aligned} E_k(n,q) =& \frac{1}{q}\sum_{c=1}^{q-1} e\left(\frac{-cn}{q}\right) \sum_{\substack{a=1 \\ a\in G}}^{q-1} e\left(\frac{ac}{q}\right) \sum_{\substack{b=1 \\ b\in R_k}}^{q-1} e\left(\frac{bc}{q}\right) \\ =& \frac{1}{kq}\sum_{c=1}^{q-1} e\left(\frac{-cn}{q}\right) \sum_{\substack{a=1 \\ a\in G}}^{q-1} e\left(\frac{ac}{q}\right) \sum_{b=1}^{q-1} \left(1 + \chi_k(b) + \chi_k^2(b) + \cdots + \chi_k^{k-1}(b)\right) \\ & \times e\left(\frac{bc}{q}\right) \\ =& -\frac{\phi(\phi(q))}{kq\phi(q)} \sum_{c=1}^{q-1} e\left(\frac{-cn}{q}\right) \sum_{a=1}^{q-1} \sum_{d|\phi(q)} \frac{\mu(d)}{\phi(d)} \sum_{\substack{h=1 \\ (h,d)=1}}^{d} e\left(\frac{h\ ind\ a}{d}\right) e\left(\frac{ac}{q}\right) \end{aligned} \tag{5}$$

$$
\begin{aligned}
&+\frac{\phi(\phi(q))}{kq\phi(q)}\sum_{c=1}^{q-1}e\left(\frac{-cn}{q}\right)\sum_{a=1}^{q-1}\sum_{d|\phi(q)}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d}e\left(\frac{h\ ind\ a}{d}\right)e\left(\frac{ac}{q}\right)\\
&\quad\times\sum_{b=1}^{q-1}\sum_{i=1}^{k-1}\chi_k^i(b)e\left(\frac{bc}{q}\right)\\
&\equiv M_1+M_2, \qquad (6)
\end{aligned}
$$

where χ_k denotes the k-th order Dirichlet character modulo q. In fact, the map which takes a with $(a,q)=1$ to $e\left(\frac{h\ ind\ a}{d}\right)$ is a Dirichlet character modulo q with order d. We shall denote this by $\chi_{h,d}(a)$. Thus, from (6) we have

$$
\begin{aligned}
|M_1| &= \left|-\frac{1}{kq}\sum_{c=1}^{q-1}e\left(\frac{-cn}{q}\right)\sum_{d|\phi(q)}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d}\sum_{a=1}^{q-1}\chi_{h,d}(a)e\left(\frac{ac}{q}\right)\right|\\
&= \left|\frac{\phi(\phi(q))}{kq\phi(q)}\left(\sum_{c=1}^{q}e\left(\frac{c(a-n)}{q}\right)-1\right)\sum_{d|\phi(q)}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d}\sum_{a=1}^{q-1}\chi_{h,d}(a)\right|\\
&= \frac{\phi(\phi(q))}{k\phi(q)}\left|\sum_{d|\phi(q)}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d}\chi_{h,d}(n)\right|\\
&\le \frac{\phi(\phi(q))}{k\phi(q)}\sum_{d|\phi(q)}\frac{|\mu(d)|}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d}1\\
&\le \frac{\phi(\phi(q))}{k\phi(q)}2^{\omega(\phi(q))}, \qquad (7)
\end{aligned}
$$

and

$$
\begin{aligned}
M_2 &= \frac{\phi(\phi(q))}{kq\phi(q)}\sum_{c=1}^{q-1}e\left(\frac{-cn}{q}\right)\sum_{d|\phi(q)}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d}\chi_{h,d}(a)e\left(\frac{ac}{q}\right)\\
&\quad\times\sum_{b=1}^{q-1}\sum_{i=1}^{k-1}\chi_k^i(b)e\left(\frac{bc}{q}\right)\\
&= \frac{\phi(\phi(q))}{kq\phi(q)}\sum_{d|\phi(q)}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d}\sum_{a=1}^{q-1}\chi_{h,d}(a)\sum_{i=1}^{k-1}\sum_{b=1}^{q-1}\chi_k^i(b)\\
&\quad\times\left(\sum_{c=1}^{q}e\left(\frac{c(a+b-n)}{q}\right)-1\right)
\end{aligned}
$$

$$=\frac{\phi(\phi(q))}{k\phi(q)}\sum_{d|\phi(q)}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d}\sum_{i=1}^{k-1}\sum_{b=1}^{q-1}\chi_{h,d}(n-b)\chi_k^i(b)$$

$$=\frac{\phi(\phi(q))}{k\phi(q)}\sum_{d|\phi(q)}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d}\sum_{i=1}^{k-1}J(n,\chi_{h,d},\chi_k^i,q). \tag{8}$$

The Jacobi sums $J(n,\chi_{h,d},\chi_k^i,q)$ satisfies Lemma 2 for some h,d,i,k. Thus,

$$|M_2|\le\frac{\phi(\phi(q))}{k\phi(q)}\sum_{d|\phi(q)}\frac{|\mu(d)|}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d}\sum_{i=1}^{k-1}|J(n,\chi_{h,d},\chi_k^i,q)|$$

$$\le\frac{(k-1)\phi(\phi(q))}{k\phi(q)}2^{\omega(\phi(q))}qp^{-\frac{1}{2}}. \tag{9}$$

Combining (4), (6), (7) and (9) we obtain

$$N_k(n,q)=\frac{\phi(\phi(q))\phi(q)}{kq}+\xi\frac{\phi(\phi(q))}{\phi(q)}2^{\omega(\phi(q))}qp^{-\frac{1}{2}},$$

where $|\xi|\le 1$.

This completes the proof of Theorem 1. □

Proof of Theorem 2 From (5) and (3), we have

$$\sum_{n=1}^{p}E_2^2(n,p)=\frac{1}{p^2}\sum_{c_1=1}^{p-1}\sum_{c_2=1}^{p-1}\left(\sum_{\substack{a_1=1\\a_1\in G}}^{p-1}e\left(\frac{a_1c_1}{p}\right)\right)\left(\sum_{\substack{a_2=1\\a_2\in G}}^{p-1}e\left(\frac{a_2c_2}{p}\right)\right)$$

$$\times\left(\sum_{\substack{b_1=1\\b_1\in R_2}}^{p-1}e\left(\frac{b_1c_1}{p}\right)\right)\left(\sum_{\substack{b_2=1\\b_2\in R_2}}^{p-1}e\left(\frac{b_2c_2}{p}\right)\right)\sum_{n=1}^{p}e\left(\frac{n(-c_1-c_2)}{p}\right)$$

$$=\frac{1}{p}\sum_{c=1}^{p-1}\left|\sum_{\substack{a=1\\a\in G}}^{p-1}e\left(\frac{ac}{p}\right)\right|^2\cdot\left|\sum_{\substack{b=1\\b\in R_2}}^{p-1}e\left(\frac{bc}{p}\right)\right|^2$$

$$=\frac{1}{4p}\sum_{c=1}^{p-1}\left|\sum_{\substack{a=1\\a\in G}}^{p-1}e\left(\frac{ac}{p}\right)\right|^2\cdot\left|\sum_{b=1}^{p-1}\left(1+\left(\frac{b}{p}\right)\right)e\left(\frac{bc}{p}\right)\right|^2$$

$$=\frac{1}{4p}\sum_{c=1}^{p-1}\left|\sum_{\substack{a=1\\a\in G}}^{p-1}e\left(\frac{ac}{p}\right)\right|^2\cdot\left|\left(\frac{c}{p}\right)\tau(\chi_2)-1\right|^2,$$

where $\tau(\chi_2)=\sum_{b=1}^{p}\left(\frac{b}{p}\right)e\left(\frac{b}{p}\right)$ is the Gauss sum related to the Legendre symbol $\chi_2=\left(\frac{\cdot}{p}\right)$.

Noting that $|\tau(\chi_2)|^2 = p$, then

$$\begin{aligned}\sum_{n=1}^{p} E^2(n,p) &= \frac{1}{4p}\sum_{c=1}^{p-1}\left|\sum_{\substack{a=1\\a\in G}}^{p-1} e\left(\frac{ac}{p}\right)\right|^2 \cdot \left(p+1-2\left(\frac{c}{p}\right)\tau(\chi_2)\right)\\ &= \frac{p+1}{4p}\sum_{c=1}^{p-1}\left|\sum_{\substack{a=1\\a\in G}}^{p-1} e\left(\frac{ac}{p}\right)\right|^2 - \frac{\tau(\chi_2)}{2p}\sum_{c=1}^{p-1}\left(\frac{c}{p}\right)\left|\sum_{\substack{a=1\\a\in G}}^{p-1} e\left(\frac{ac}{p}\right)\right|^2\\ &= \frac{p+1}{4p}(p\phi(p-1)-\phi^2(p-1)) - \frac{\tau(\chi_2)}{2p}\sum_{c=1}^{p-1}\left(\frac{c}{p}\right)\left|\sum_{\substack{a=1\\a\in G}}^{p-1} e\left(\frac{ac}{p}\right)\right|^2. \end{aligned} \tag{10}$$

Now we estimate the second term in (10). Due to Lemma 1, we have

$$\begin{aligned}&\frac{\tau(\chi_2)}{2p}\sum_{c=1}^{p-1}\left(\frac{c}{p}\right)\left|\sum_{\substack{a=1\\a\in G}}^{p-1} e\left(\frac{ac}{p}\right)\right|^2\\ &= \frac{\tau(\chi_2)}{2p}\sum_{c=1}^{p-1}\left(\frac{c}{p}\right)\left|\sum_{a=1}^{p-1}\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d} e\left(\frac{h\,ind\,a}{d}\right)e\left(\frac{ac}{p}\right)\right|^2\\ &= \frac{\tau(\chi_2)}{2p}\sum_{c=1}^{p-1}\left(\frac{c}{p}\right)\left|\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d}\sum_{a=1}^{p-1}\chi_{h,d}(a)e\left(\frac{ac}{p}\right)\right|^2\\ &= \frac{\tau(\chi_2)}{2p}\sum_{c=1}^{p-1}\left(\frac{c}{p}\right)\left|\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{\substack{h=1\\(h,d)=1}}^{d}\overline{\chi}_{h,d}(c)\tau(\chi_{h,d})\right|^2\\ &= \frac{\tau(\chi_2)}{2p}\sum_{d_1|p-1}\sum_{d_2|p-1}\frac{\mu(d_1)\mu(d_2)}{\phi(d_1)\phi(d_2)}\sum_{\substack{h_1=1\\(h_1,d_1)=1}}^{d_1}\sum_{\substack{h_2=1\\(h_2,d_2)=1}}^{d_2}\tau(\overline{\chi}_{h_1,d_1})\tau(\chi_{h_2,d_2})\\ &\quad\times\sum_{c=1}^{p-1}\left(\frac{c}{p}\right)\overline{\chi}_{h_1,d_1}(c)\chi_{h_2,d_2}(c). \end{aligned} \tag{11}$$

Let $\chi'_{h_1,h_2,d_1,d_2}(c) = \left(\frac{c}{p}\right)\overline{\chi}_{h_1,d_1}(c)\chi_{h_2,d_2}(c)$. It is clear that χ'_{h_1,h_2,d_1,d_2} is a Dirichlet character modulo p. If χ'_{h_1,h_2,d_1,d_2} is principal, then we have

$$\sum_{c=1}^{p-1}\chi'_{h_1,h_2,d_1,d_2}(c) = p-1.$$

Thus, we have the following estimate

$$\left|\frac{\tau(\chi_2)}{2p}\sum_{c=1}^{p-1}\left(\frac{c}{p}\right)\left|\sum_{\substack{a=1\\a\in G}}^{p-1}e\left(\frac{ac}{p}\right)\right|^2\right| \le 2^{2\omega(p-1)}p^{\frac{3}{2}}, \tag{12}$$

where we used the fact $|\tau(\chi)| = \sqrt{p}$ if χ is a non-principal character modulo p. Then, combining (10) and (12), we have Theorem 2. □

References

1. J. Cilleruelo, A. Zumalacárregui An additive problem in finite fields with powers of elements of large multiplicative order *Revista Matemática Complutense* **27** 2014 501-508
2. S. D. Cohen, G. L. Mullen Primitive elements in Costas arrays *Applicable Algebra in Engineering, Communication and Computing* **2** 1991 45-53
3. S. D. Cohen, W. P. Zhang Sums of two exact powers *Finite Fields and Their Applications* **8** 2002 471-477
4. M. Z. Garaev, Ka-Lam Kueh Distribution of special sequences modulo a large prime *International Journal of Mathematics and Mathematical Sciences* **50** 2003 3189-3194
5. C. V. Garcia A note on an additive problem with powers of a primitive root *Boletín de la Sociedad Matemaática Mexicana* **11** 2005 1-4
6. S. Golomb On the algebra construction for Costas arrays *Journal of Combinational Theory (Series A.)* **37** 1984 13-21
7. M. Long, V. Pigno, C. Pinner Evaluating prime power Gauss and Jacobi sums *Tamkang Journal of Mathematics* **48** 2017 227-240
8. W. Narkiewicz Classical problems in number theory PWN Polish Scientific Publishers Warszawa 1987 79-80
9. V. Pigno, C. Pinner Binomial character sums modulo prime powers *Journal Théorie des Nombres de Bordeaux* **28** 2016 39-53
10. Z. Rudnik, A. Zaharescu The distribution of spacings between small powers of a primitive root *Israel Journal of Mathematics* **120** 2000 271-287
11. J. Wang On the Jacobi sums modulo P^n *Journal of Number Theory* **28** 1991 50-64
12. W. P. Zhang On the primitive roots and the quadratic residues modulo p *Studia Scientiarum Mathematicarum Hungarica* **35** 1999 139-145

Authors and Affiliations

Zhefeng Xu[1] · Jiankang Wang[1]

✉ Zhefeng Xu
zfxu@nwu.edu.cn

[1] School of Mathematics, Northwest University, Xi'an, Shaanxi, P.R. China