AIMS Mathematics, 5(6): 5654–5663.
DOI:10.3934/math.2020361
Received: 30 April 2020
Accepted: 22 June 2020
Published: 02 July 2020

http://www.aimspress.com/journal/Math

Research article

On the primitive roots and the generalized Golomb's conjecture

Jiafan Zhang and Xingxing Lv*

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

* **Correspondence:** Email: lvxingxing@stumail.nwu.edu.cn.

Abstract: In this article, we use elementary methods and the estimate for character sums to study the properties of a certain primitive roots modulo p (an odd prime), and prove that the generalized Golomb's conjecture is correct in a reduced residue system modulo p. This solved an open problem proposed by W. P. Zhang and T. T. Wang in [3].

Keywords: primitive roots; the estimate for character sums; the generalized Golomb's conjecture; square-free number
Mathematics Subject Classification: 11A07, 11D85

1. Introduction

Let p be an odd prime, $\mathbb{F}_q$ denotes a finite field of q elements with characteristic p. When S. W. Golomb studied some combinatorial problems in [1], he proposed the following two interesting problems:

(A). Whether there exist two primitive elements $\alpha, \beta \in \mathbb{F}_q$ such that the equation $\alpha + \beta = 1$ holds?

(B). For $q > 3$, whether there exist two primitive elements $\alpha, \beta \in \mathbb{F}_q$ such that the equation $\alpha+\beta = -1$ holds?

These two problems have now been basically solved, at the same time, they have also been generalized and extended. Some papers related to primitive roots and Golomb conjecture can be found in [2–16]. For example, Sun Qi [2] proved the following generalized result:

Let integer $q = p^n$ be a power of prime p. If q is large enough, then for any non-zero elements $a, b, c \in \mathbb{F}_q$, there exist two primitive elements $\alpha, \beta \in \mathbb{F}_q$ such that the equation $a\alpha + b\beta = c$ holds.

Formally, Golomb conjecture has been basically solved, and therefore there is no work to do in this area. But that is not the case, there is still room for further discussion. In fact recently, W. P. Zhang and T. T. Wang [3] further extended Golomb's conjecture in a reduced residue system modulo p, and proved the following stronger result:

Let p be an odd prime large enough. Then for any integers $1 \le a \ne b \le p-1$, there exist three primitive roots α, β and γ modulo p such that the congruence equations $\alpha+\gamma \equiv a \bmod p$ and $\beta+\gamma \equiv b \bmod p$ hold.

It is not difficult to see from the methods in [3] that the above result can also be further extended to the following forms:

Let p be an odd prime large enough, u_i and v_i are integers with $(u_1u_2v_1v_2, p) = 1$. Then for any integers $1 \leq a \neq b \leq p-1$, there exist three primitive roots α, β and γ modulo p such that the congruence equations

$$u_1\alpha + v_1\gamma \equiv a \bmod p \ \text{ and } \ u_2\beta + v_2\gamma \equiv b \bmod p \ \text{ hold.}$$

In fact, the above result can be generalized to an arbitrary finite field $\mathbb{F}_q$. That is, for any non-zero elements $u_i, v_i, a, b \in \mathbb{F}_q$, there exist three primitive elements $\alpha, \beta, \gamma \in \mathbb{F}_q$ such that the equation $u_1\alpha + v_1\gamma = a$, $u_2\beta + v_2\gamma = b$ holds.

In W. P. Zhang and T. T. Wang [3], they also proposed the following open problem: Can the Golomb conjecture be extended further?

Specifically, for three distinct nonzero elements a, b and $c \in \mathbb{F}_q$, do there exist four primitive elements α, β, γ and $\delta \in \mathbb{F}_q$, such that the equations

$$\alpha + \delta = a, \ \ \beta + \delta = b \ \text{ and } \ \gamma + \delta = c \ \text{ are satisfied ?}$$

Obviously, the result in [3] is very meaningful. It not only gives us a stronger conclusion than Golomb's conjecture, but also points out the direction of further research. At the same time, we will naturally consider more general problem:

For any k (≥ 2) nonzero elements $c_i \in \mathbb{F}_q$ ($i = 1, 2, \cdots, k$), do there exist $k+1$ primitive elements α_i and $\beta \in \mathbb{F}_q$ ($i = 1, 2, \cdots, k$), such that the equations

$$\alpha_i + \beta = c_i, \ \ i = 1, 2, \cdots, k \ ?$$

Through careful reading of [3], we find that the reason why the authors were unable to prove the general case is that they used the properties of the classical Gauss sums, which resulted in one kind of character sums that can not be optimally estimated. That is, they can not get the estimate

$$\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}\chi_1(a)\chi_2(b)\chi_3(a+1)\chi_4(b+1)\chi_5(ca+db+1) \ll p,$$

where c and d are constants, and $\chi_1, \chi_2, \cdots, \chi_5$ denote the Dirichlet characters modulo p, at least one of which is non-principal character.

In this paper, we make up for the deficiency in [3] and avoid using the classical Gauss sums. Thus, the open problem in [3] is solved, and the more general conclusion is proved. For ease of statement, we will rewrite the problem in [3] in another form: Let p be an odd prime, k be any fixed positive integer. Then for any k different integers $c_1, c_2, \cdots, c_k \in \{1, 2, \cdots, p-1\}$, whether there exists an integer a modulo p such that $a, c_1 - a, c_2 - a, \cdots, c_k - a$ are all primitive roots modulo p? where the condition that c_i are non-zero is necessary. Otherwise, there is no guarantee that a and $-a$ are both primitive roots modulo p.

If so, let $N(c_1, c_2, \cdots, c_k; p)$ denotes the number of all such $1 \leq a \leq p-1$. What about the asymptotic properties of $N(c_1, c_2, \cdots, c_k; p)$?

Similarly, we can also let $M(c_1, c_2, \cdots, c_k; p)$ denotes the number of all $1 \leq a \leq p-1$ such that a is a square-free (i.e., $d^2 \mid a$ if and only if $d = 1$) primitive root modulo p, $c_1 - a, c_2 - a, \cdots, c_k - a$ are all primitive roots modulo p.

L. Carlitz [21] proved that some properties of $N(c_1, c_2, \cdots, c_k; p)$ depends on some results of Davenport.

This paper as a note of [1] and [3], we will use elementary methods and the estimate for character sums to study the asymptotic properties of $N(c_1, c_2, \cdots, c_k; p)$ and $M(c_1, c_2, \cdots, c_k; p)$, and give two sharp asymptotic formulas for them. That is, we have the following results:

Theorem 1. Let p be an odd prime, k be a fixed positive integer. Then for any k different integers $c_1,\ c_2, \cdots, c_k \in \{1, 2, 3, \cdots, p-1\}$, we have

$$N(c_1, c_2, \cdots, c_k; p) = \frac{\phi^{k+1}(p-1)}{(p-1)^k} + O_k\left(\frac{\phi^{k+1}(p-1)}{p^{k+\frac{1}{2}}} \cdot 2^{(k+1)\cdot\omega(p-1)}\right),$$

where $\phi(n)$ is the Euler function, and $\omega(n)$ denotes the number of all distinct prime divisors of n, O_k denotes the big-O constant depend only on k.

Theorem 2. Let p be an odd prime, k be a fixed positive integer. Then for any k different integers $c_1,\ c_2, \cdots, c_k \in \{1, 2, 3, \cdots, p-1\}$, we have

$$M(c_1, c_2, \cdots, c_k; p) = \frac{6}{\pi^2} \cdot \frac{\phi^{k+1}(p-1)}{(p-1)^k} + O_k\left(\frac{\phi^{k+1}(p-1)}{p^{k+\frac{1}{4}}} \cdot \sqrt{\ln p} \cdot 2^{(k+1)\cdot\omega(p-1)}\right).$$

It is easy to prove that our theorems also hold in the finite field $\mathbb{F}_q$. From our theorems we may immediately deduce a generalized results of [1] and [3]. That is, we have the following two corollaries:

Corollary 1. Let p be a prime large enough, k be a fixed positive integer. Then for any k different non-zero elements $c_1,\ c_2, \cdots, c_k \in \mathbb{F}_p$, there exist $k+1$ primitive elements $\alpha_1, \alpha_2, \cdots, \alpha_k, \beta \in \mathbb{F}_p$ such that all equations

$$\alpha_1 + \beta = c_1,\ \alpha_2 + \beta = c_2,\ \cdots,\ \alpha_k + \beta = c_k \text{ hold.}$$

Corollary 2. Let p be a prime large enough, k be a fixed positive integer. Then for any k different integers $c_1,\ c_2, \cdots, c_k \in \{1, 2, 3, \cdots, p-1\}$, there exist k primitive roots $\alpha_1, \alpha_2, \cdots, \alpha_k$ and a square-free primitive root β modulo p such that all congruence equations

$$\alpha_1 + \beta \equiv c_1 \bmod p,\ \alpha_2 + \beta \equiv c_2 \bmod p,\ \cdots,\ \alpha_k + \beta \equiv c_k \bmod p \text{ hold.}$$

Some notes: It is not difficult to see that our Corollary 1 not only solved the open problem ($k = 3$) proposed by W. P. Zhang and T. T. Wang in [3], but also obtained more general theorems. Of course, Theorem 1 can also be obtained in different ways, see C. Cobeli and A. Zaharescu [4]. These generalized results not only reveal the close relationship between the primitive elements in a finite field $\mathbb{F}_p$, but also characterize their dense properties in the finite field. The results in [1] and [3] are the special cases of our Theorem 1, i.e., $k = 1$ and $k = 2$. Theorem 2 is a general and stronger result, which means that one of the primitive roots can be a square-free number. This result has a special meaning in elementary number theory. That is to say, if p is a prime large enough, then for any primitive root $\beta \bmod p$ with $|\mu(\beta)| = 1$, there exist two primitive roots α and γ modulo p such that $\alpha \equiv \beta - \gamma \bmod p$ and $|\mu(\gamma)| = 1$.

2. Several lemmas

To complete the proofs of our main results, we need following several simple lemmas. Of course, the proofs of these lemmas require some elementary and analytic number theory knowledge. In particular,

the contents of primitive roots and Dirichlet characters modulo p are required. All these can be found in [17], we would not repeat them here. First we have the following:

Lemma 1. Let p be an odd prime, then for any integer a coprime to p (i.e., $(a, p) = 1$), we have the identity

$$\frac{\phi(p-1)}{p-1}\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{r=1}^{k}{}' e\left(\frac{r\cdot \mathrm{ind}(a)}{k}\right) = \begin{cases} 1 & \text{if } a \text{ is a primitive root mod } p; \\ 0 & \text{if } a \text{ is not a primitive root mod } p, \end{cases}$$

where $e(y) = e^{2\pi iy}$, $\sum_{r=1}^{k}{}'$ denotes the summation over all integers $1 \le r \le k$ such that r is coprime to k, $\mu(n)$ is the Möbius function, and $\mathrm{ind}(a)$ denotes the index of a relative to some fixed primitive root g mod p.

Proof. See Proposition 2.2 in [18].

Lemma 2. Let p be an odd prime, $\chi_1, \cdots, \chi_r$ be Dirichlet characters modulo p, at least one of which is non-principal character modulo p. Let $f(x)$ be an integral coefficient polynomial of degree d. Then for any r distinct integers (in the sense of congruence modulo p) $a_1, \cdots, a_r$, we have the estimate

$$\left|\sum_{a=1}^{p-1}\chi_1(a+a_1)\chi_2(a+a_2)\cdots\chi_r(a+a_r)\,e\left(\frac{f(a)}{p}\right)\right| \le (r+d)\cdot p^{\frac{1}{2}}.$$

Proof. This estimate is Lemma 17 in [19]. Its proof relies on deep results from number theory. For detailed proof, see Appendix 5, Example 12 in [20].

Lemma 3. Let p be an odd prime, k be a fixed positive integer, $\chi_1, \cdots, \chi_k$ be Dirichlet characters modulo p, at least one of which is non-principal character modulo p, N be any positive integer with $1 < N \le p-1$. Then for distinct integers $c_1, c_2, \cdots, c_k$ modulo p, we have the estimate

$$\sum_{1\le a\le N}\chi_1(a-c_1)\cdot\chi_2(a-c_2)\cdots\chi_k(a-c_k) \ll_k \sqrt{p}\cdot\ln p,$$

where $\ll_k$ denotes the big-O constant depend only on k.

Proof. If $N = p-1$, then from Lemma 2 we have the estimate

$$\left|\sum_{a=1}^{p-1}\chi_1(a-c_1)\cdot\chi_2(a-c_2)\cdots\chi_k(a-c_k)\right| \ll \sqrt{p}. \tag{2.1}$$

If $1 < N < p-1$, then from (2.1), Lemma 2, the identity

$$\sum_{r=0}^{p-1} e\left(\frac{nr}{p}\right) = \begin{cases} p & \text{if } p \mid n; \\ 0 & \text{if } p \nmid n \end{cases}$$

and the estimate

$$\left|\sum_{b\le N} e\left(\frac{-rb}{p}\right)\right| \ll \frac{1}{\left|\sin\left(\frac{r\pi}{p}\right)\right|} \ll \frac{p}{\min(r, p-r)}$$

we have

$$\sum_{1\le a\le N}\chi_1(a-c_1)\cdot\chi_2(a-c_2)\cdots\chi_k(a-c_k)$$

$$
\begin{aligned}
&= \frac{1}{p}\sum_{b=1}^{N}\sum_{1\le a\le p-1}\sum_{r=0}^{p-1}\chi_1(a-c_1)\cdot\chi_2(a-c_2)\cdots\chi_k(a-c_k)\cdot e\left(\frac{r(a-b)}{p}\right)\\
&= \frac{1}{p}\sum_{r=1}^{p-1}\left(\sum_{1\le b\le N} e\left(\frac{-rb}{p}\right)\right)\left(\sum_{a=1}^{p-1}\chi_1(a-c_1)\cdot\chi_2(a-c_2)\cdots\chi_k(a-c_k)\cdot e\left(\frac{ra}{p}\right)\right)\\
&\quad +\frac{N}{p}\sum_{a=1}^{p-1}\chi_1(a-c_1)\cdot\chi_2(a-c_2)\cdots\chi_k(a-c_k)\\
&\ll \frac{\sqrt{p}}{p}\sum_{r=1}^{p-1}\frac{1}{\left|\sin\left(\frac{r\pi}{p}\right)\right|}+\frac{N}{\sqrt{p}}\ll \sqrt{p}\sum_{r=1}^{p-1}\frac{1}{r}\ll \sqrt{p}\cdot\ln p. \qquad (2.2)
\end{aligned}
$$

Now Lemma 3 follows from the estimates (2.1) and (2.2).

Lemma 4. Let p be an odd prime, k be a fixed positive integer, $\chi_1, \cdots, \chi_k$ be Dirichlet characters modulo p, at least one of which is non-principal character. Then for pairwise distinct integers $c_1, c_2, \cdots, c_k$ modulo p, we have the estimate

$$
\sum_{a=1}^{p-1}|\mu(a)|\cdot\chi_1(a-c_1)\cdot\chi_2(a-c_2)\cdots\chi_k(a-c_k)\ll_k p^{\frac{3}{4}}\cdot\sqrt{\ln p}.
$$

Proof. Let $T = p^{\frac{1}{4}}/\sqrt{\ln p}$, note that (see Exercises for Chapter 2 in [17])

$$
|\mu(a)| = \sum_{d^2|a}\mu(d), \qquad (2.3)
$$

from (2.3) and the properties of the partition we have

$$
\begin{aligned}
&\sum_{a=1}^{p-1}|\mu(a)|\cdot\chi_1(a-c_1)\cdot\chi_2(a-c_2)\cdots\chi_k(a-c_k)\\
&= \sum_{a=1}^{p-1}\sum_{d^2|a}\mu(d)\cdot\chi_1(a-c_1)\cdot\chi_2(a-c_2)\cdots\chi_k(a-c_k)\\
&= \sum_{d^2a\le p-1}\mu(d)\cdot\chi_1\left(ad^2-c_1\right)\cdot\chi_2\left(ad^2-c_2\right)\cdots\chi_k\left(ad^2-c_k\right)\\
&= \sum_{d\le\sqrt{p}}\mu(d)\chi_1^2(d)\chi_2^2(d)\cdots\chi_k^2(d)\sum_{a\le\frac{p}{d^2}}\prod_{i=1}^{k}\chi_i\left(a-c_i\overline{d}^2\right)\\
&= \sum_{d\le T}\mu(d)\chi_1^2(d)\chi_2^2(d)\cdots\chi_k^2(d)\sum_{a\le\frac{p}{d^2}}\prod_{i=1}^{k}\chi_i\left(a-c_i\overline{d}^2\right)\\
&\quad +\sum_{T<d\le\sqrt{p}}\mu(d)\chi_1^2(d)\chi_2^2(d)\cdots\chi_k^2(d)\sum_{a\le\frac{p}{d^2}}\prod_{i=1}^{k}\chi_i\left(a-c_i\overline{d}^2\right)\\
&\equiv V_1+V_2. \qquad (2.4)
\end{aligned}
$$

Applying Lemma 3 we have the estimate

$$\begin{aligned} V_1 &= \sum_{d\le T}\mu(d)\chi_1^2(d)\chi_2^2(d)\cdots\chi_k^2(d)\sum_{a\le\frac{p}{d^2}}\prod_{i=1}^{k}\chi_i\left(a-c_i\overline{d}^2\right)\\ &\ll \sum_{d\le T}|\mu(d)|\cdot\sqrt{p}\cdot\ln p \ll T\cdot\sqrt{p}\cdot\ln p. \end{aligned} \tag{2.5}$$

From the trivial estimate we also have

$$\begin{aligned} V_2 &= \sum_{T<d\le\sqrt{p}}\mu(d)\chi_1^2(d)\chi_2^2(d)\cdots\chi_k^2(d)\sum_{a\le\frac{p}{d^2}}\prod_{i=1}^{k}\chi_i\left(a-c_i\overline{d}^2\right)\\ &\ll \sum_{T<d\le\sqrt{p}}|\mu(d)|\cdot\frac{p}{d^2}\ll\frac{p}{T}. \end{aligned} \tag{2.6}$$

Combining (2.4), (2.5) and (2.6) we have the estimate

$$\sum_{a=1}^{p-1}|\mu(a)|\cdot\chi_1(a-c_1)\cdot\chi_2(a-c_2)\cdots\chi_k(a-c_k)\ll p^{\frac{3}{4}}\cdot\sqrt{\ln p}.$$

This proves Lemma 4.

3. Proofs of the theorems

In this part, we shall prove our main results. First we prove Theorem 1. Let p be an odd prime, k be any fixed positive integer. Then for any k different integers $c_1,\ c_2,\cdots,c_k\in\{1,2,3,\cdots,p-1\}$, from Lemma 1 we have

$$\begin{aligned} N(c_1,c_2,\cdots,c_k;p) &= \frac{\phi^{k+1}(p-1)}{(p-1)^{k+1}}\sum_{\substack{a=1\\ a\ne c_i,i=1,2,\cdots k}}^{p-1}\left(\sum_{h|p-1}\frac{\mu(h)}{\phi(h)}\sideset{}{'}\sum_{s=1}^{h}e\left(\frac{s\cdot\mathrm{ind}(a)}{h}\right)\right)\\ &\times\prod_{i=1}^{k}\left(\sum_{h_i|p-1}\frac{\mu(h_i)}{\phi(h_i)}\sideset{}{'}\sum_{s_i=1}^{h_i}e\left(\frac{s_i\cdot\mathrm{ind}(c_i-a)}{h_i}\right)\right). \end{aligned} \tag{3.1}$$

For any integer $1\le s\le h\le p-1$ with $h\mid p-1$ and $(s,h)=1$, we write $e\left(\frac{s\cdot\mathrm{ind}(a)}{h}\right)=\chi_{s,h}(a)$, and $\chi_{s,h}(a)=0$, if $p\mid a$. It is clear that $\chi_{s,h}(a)$ is a Dirichlet character modulo p, $\chi_{1,1}=\chi_0$ denotes the principal character modulo p. So from (3.1) and the above notations we have

$$\begin{aligned} N(c_1,c_2,\cdots,c_k;p) &= \frac{\phi^{k+1}(p-1)}{(p-1)^{k+1}}\sum_{h|p-1}\frac{\mu(h)}{\phi(h)}\sideset{}{'}\sum_{s=1}^{h}\sum_{h_1|p-1}\frac{\mu(h_1)}{\phi(h_1)}\sideset{}{'}\sum_{s_1=1}^{h_1}\\ &\cdots\sum_{h_k|p-1}\frac{\mu(h_k)}{\phi(h_k)}\sideset{}{'}\sum_{s_k=1}^{h_k}\sum_{a=1}^{p-1}\chi_{s,h}(a)\chi_{s_1,h_1}(c_1-a)\cdot\chi_{s_2,h_2}(c_2-a)\cdots\chi_{s_k,h_k}(c_k-a)\\ &= \frac{\phi^{k+1}(p-1)}{(p-1)^{k+1}}\sum_{a=1}^{p-1}\chi_0(a)\chi_0(c_1-a)\cdot\chi_0(c_2-a)\cdots\chi_0(c_k-a) \end{aligned}$$

$$+\frac{\phi^{k+1}(p-1)}{(p-1)^{k+1}}\sum_{\substack{h|p-1\\(h,h_1,h_2,\cdots,h_k)\neq(1,1,1,\cdots,1)}}\sum_{h_1|p-1}\cdots\sum_{h_k|p-1}\frac{\mu(h)}{\phi(h)}\cdot\frac{\mu(h_1)}{\phi(h_1)}\cdot\frac{\mu(h_2)}{\phi(h_2)}\cdots\frac{\mu(h_k)}{\phi(h_k)}$$
$$\times\sum_{s=1}^{h}{}'\sum_{s_1=1}^{h_1}{}'\cdots\sum_{s_k=1}^{h_k}{}'\sum_{a=1}^{p-1}\chi_{s,h}(a)\chi_{s_1,h_1}(c_1-a)\cdots\chi_{s_k,h_k}(c_k-a)$$
$$\equiv W_1+W_2. \tag{3.2}$$

Now we estimate W_1 and W_2 in (3.2) respectively. It is clear that

$$\begin{aligned}W_1 &= \frac{\phi^{k+1}(p-1)}{(p-1)^{k+1}}\sum_{a=1}^{p-1}\chi_0(a)\chi_0(c_1-a)\chi_0(c_2-a)\cdots\chi_0(c_k-a)\\ &= \frac{\phi^{k+1}(p-1)}{(p-1)^{k}}+O\left(\frac{\phi^{k+1}(p-1)}{(p-1)^{k+1}}\cdot k\right).\end{aligned} \tag{3.3}$$

Note that if $(h,h_1,h_2,\cdots,h_k)\neq(1,1,1,\cdots,1)$, then at least one of $\chi_{s,h},\chi_{s_1,h_1},\chi_{s_2,h_2},\cdots,\chi_{s_k,h_k}$ is not principal character modulo p. Then from the identity

$$\sum_{d|n}\frac{|\mu(d)|}{\phi(d)}\sum_{r=1}^{d}{}'1=\sum_{d|n}|\mu(d)|=\prod_{p^\alpha\|n}\left(\sum_{r|p^\alpha}|\mu(r)|\right)=\prod_{p^\alpha\|n}(1+1)=2^{\omega(n)} \tag{3.4}$$

and Lemma 2 we have the estimate

$$\begin{aligned}W_2 &= \frac{\phi^{k+1}(p-1)}{(p-1)^{k+1}}\sum_{\substack{h|p-1\\(h,h_1,h_2,\cdots,h_k)\neq(1,1,1,\cdots,1)}}\sum_{h_1|p-1}\cdots\sum_{h_k|p-1}\frac{\mu(h)}{\phi(h)}\cdot\frac{\mu(h_1)}{\phi(h_1)}\cdot\frac{\mu(h_2)}{\phi(h_2)}\cdots\frac{\mu(h_k)}{\phi(h_k)}\\ &\quad\times\sum_{s=1}^{h}{}'\sum_{s_1=1}^{h_1}{}'\cdots\sum_{s_k=1}^{h_k}{}'\sum_{a=1}^{p-1}\chi_{s,h}(a)\chi_{s_1,h_1}(c_1-a)\cdots\chi_{s_k,h_k}(c_k-a)\\ &\ll \frac{\phi^{k+1}(p-1)}{(p-1)^{k+1}}\sum_{\substack{h|p-1\\(h,h_1,h_2,\cdots,h_k)\neq(1,1,1,\cdots,1)}}\sum_{h_1|p-1}\cdots\sum_{h_k|p-1}\frac{|\mu(h)|}{\phi(h)}\cdot\frac{|\mu(h_1)|}{\phi(h_1)}\cdot\frac{|\mu(h_2)|}{\phi(h_2)}\cdots\frac{|\mu(h_k)|}{\phi(h_k)}\\ &\quad\times\sum_{s=1}^{h}{}'\sum_{s_1=1}^{h_1}{}'\cdots\sum_{s_k=1}^{h_k}{}'\left|\sum_{a=1}^{p-1}\chi_{s,h}(a)\chi_{s_1,h_1}(c_1-a)\cdots\chi_{s_k,h_k}(c_k-a)\right|\\ &\ll \frac{\phi^{k+1}(p-1)}{(p-1)^{k+1}}\sum_{s|p-1}|\mu(s)|\sum_{s_1|p-1}|\mu(s_1)|\sum_{s_2|p-1}|\mu(s_2)|\cdots\sum_{s_k|p-1}|\mu(s_k)|\sqrt{p}\\ &\ll \frac{\phi^{k+1}(p-1)}{p^{k+\frac{1}{2}}}\cdot 2^{(k+1)\cdot\omega(p-1)}.\end{aligned} \tag{3.5}$$

Combining (3.2), (3.3), (3.4) and (3.5) we have the asymptotic formula

$$N(c_1,c_2,\cdots,c_k;p)=\frac{\phi^{k+1}(p-1)}{(p-1)^k}+O\left(\frac{\phi^{k+1}(p-1)}{p^{k+\frac{1}{2}}}\cdot 2^{(k+1)\cdot\omega(p-1)}\right).$$

This proves Theorem 1.

Now we prove Theorem 2. From the method of proving (3.2) we have the identity

$$\begin{aligned}
& M(c_1, c_2, \cdots, c_k; p) \\
= & \frac{\phi^{k+1}(p-1)}{(p-1)^{k+1}} \sum_{h|p-1} \frac{\mu(h)}{\phi(h)} \sideset{}{'}\sum_{s=1}^{h} \sum_{h_1|p-1} \frac{\mu(h_1)}{\phi(h_1)} \sideset{}{'}\sum_{s_1=1}^{h_1} \cdots \sum_{h_k|p-1} \frac{\mu(h_k)}{\phi(h_k)} \sideset{}{'}\sum_{s_k=1}^{h_k} \\
& \times \sum_{a=1}^{p-1} |\mu(a)| \cdot \chi_{s,h}(a) \chi_{s_1,h_1}(c_1 - a) \cdot \chi_{s_2,h_2}(c_2 - a) \cdots \chi_{s_k,h_k}(c_k - a) \\
= & \frac{\phi^{k+1}(p-1)}{(p-1)^{k+1}} \sum_{a=1}^{p-1} |\mu(a)| \cdot \chi_0(a) \chi_0(c_1 - a) \cdot \chi_0(c_2 - a) \cdots \chi_0(c_k - a) \\
& + \frac{\phi^{k+1}(p-1)}{(p-1)^{k+1}} \sum_{\substack{h|p-1 \\ (h,h_1,h_2,\cdots,h_k) \neq (1,1,1,\cdots,1)}} \sum_{h_1|p-1} \cdots \sum_{h_k|p-1} \frac{\mu(h)}{\phi(h)} \cdot \frac{\mu(h_1)}{\phi(h_1)} \cdot \frac{\mu(h_2)}{\phi(h_2)} \cdots \frac{\mu(h_k)}{\phi(h_k)} \\
& \times \sum_{s=1}^{h} \sideset{}{'}\sum \sum_{s_1=1}^{h_1} \sideset{}{'}\sum \cdots \sum_{s_k=1}^{h_k} \sideset{}{'}\sum \sum_{a=1}^{p-1} |\mu(a)| \cdot \chi_{s,h}(a) \chi_{s_1,h_1}(c_1 - a) \cdots \chi_{s_k,h_k}(c_k - a) \\
\equiv & E_1 + E_2. \qquad (3.6)
\end{aligned}$$

From (2.3) and properties of the Möbius function we have the asymptotic formula

$$\begin{aligned}
& \sum_{a=1}^{p-1} |\mu(a)| \cdot \chi_0(a) \chi_0(c_1 - a) \cdot \chi_0(c_2 - a) \cdots \chi_0(c_k - a) \\
= & \sum_{a=1}^{p-1} |\mu(a)| + O(k) = p \cdot \sum_{d=1}^{+\infty} \frac{\mu(d)}{d^2} + O(\sqrt{p}) = \frac{6}{\pi^2} \cdot p + O(\sqrt{p}). \qquad (3.7)
\end{aligned}$$

From (3.4) and Lemma 4 we have the estimate

$$\begin{aligned}
E_2 = & \frac{\phi^{k+1}(p-1)}{(p-1)^{k+1}} \sum_{\substack{h|p-1 \\ (h,h_1,h_2,\cdots,h_k) \neq (1,1,1,\cdots,1)}} \sum_{h_1|p-1} \cdots \sum_{h_k|p-1} \frac{\mu(h)}{\phi(h)} \cdot \frac{\mu(h_1)}{\phi(h_1)} \cdot \frac{\mu(h_2)}{\phi(h_2)} \cdots \frac{\mu(h_k)}{\phi(h_k)} \\
& \times \sum_{s=1}^{h} \sideset{}{'}\sum \sum_{s_1=1}^{h_1} \sideset{}{'}\sum \cdots \sum_{s_k=1}^{h_k} \sideset{}{'}\sum \sum_{a=1}^{p-1} |\mu(a)| \cdot \chi_{s,h}(a) \chi_{s_1,h_1}(c_1 - a) \cdots \chi_{s_k,h_k}(c_k - a) \\
\ll & \frac{\phi^{k+1}(p-1)}{(p-1)^{k+1}} \sum_{\substack{h|p-1 \\ (h,h_1,h_2,\cdots,h_k) \neq (1,1,1,\cdots,1)}} \sum_{h_1|p-1} \cdots \sum_{h_k|p-1} \frac{|\mu(h)|}{\phi(h)} \cdot \frac{|\mu(h_1)|}{\phi(h_1)} \cdot \frac{|\mu(h_2)|}{\phi(h_2)} \cdots \frac{|\mu(h_k)|}{\phi(h_k)} \\
& \times \sum_{s=1}^{h} \sideset{}{'}\sum \sum_{s_1=1}^{h_1} \sideset{}{'}\sum \cdots \sum_{s_k=1}^{h_k} \sideset{}{'}\sum \left| \sum_{a=1}^{p-1} |\mu(a)| \cdot \chi_{s,h}(a) \chi_{s_1,h_1}(c_1 - a) \cdots \chi_{s_k,h_k}(c_k - a) \right| \\
\ll & \frac{\phi^{k+1}(p-1)}{p^{k+1}} \sum_{s|p-1} |\mu(s)| \sum_{s_1|p-1} |\mu(s_1)| \cdots \sum_{s_k|p-1} |\mu(s_k)| \cdot p^{\frac{3}{4}} \cdot \sqrt{\ln p}
\end{aligned}$$

$$\ll \frac{\phi^{k+1}(p-1)}{p^{k+\frac{1}{4}}} \cdot \sqrt{\ln p} \cdot 2^{(k+1)\cdot\omega(p-1)}. \tag{3.8}$$

Combining (3.6), (3.7) and (3.8) we have the asymptotic formula

$$M(c_1, c_2, \cdots, c_k; p) = \frac{6}{\pi^2} \cdot \frac{\phi^{k+1}(p-1)}{(p-1)^k} + O\left(\frac{\phi^{k+1}(p-1)}{p^{k+\frac{1}{4}}} \cdot \sqrt{\ln p} \cdot 2^{(k+1)\cdot\omega(p-1)}\right).$$

This proves Theorem 2.

To prove Corollary 1, we assume that p is a prime large enough, k is a fixed positive integer. Then for any k different integers $c_1,\ c_2, \cdots, c_k \in \{1, 2, 3, \cdots, p-1\}$, from Theorem 1 we know that $N(c_1, c_2, \cdots, c_k; p) > 0$. So there is at least one primitive root β modulo p such that all $c_1 - \beta$, $c_2 - \beta$, $\cdots$, $c_k - \beta$ are primitive roots modulo p. Let $\alpha_i \equiv c_i - \beta \bmod p$, it is clear that all α_i are primitive roots modulo p, $i = 1, 2, \cdots, k$. Therefore, we have the congruence equations

$$\alpha_1 + \beta \equiv c_1 \bmod p,\ \alpha_2 + \beta \equiv c_2 \bmod p,\ \cdots,\ \alpha_k + \beta \equiv c_k \bmod p.$$

This proves Corollary 1.

Similarly, we can also deduce Corollary 2.

4. Conclusion

In this article, we proved two main results, they are closely related to Golomb's conjecture. Theorem 1 describes that when the prime p is large enough, then for any fixed positive integer k and any k different non-zero elements $c_1,\ c_2, \cdots, c_k \in \mathbb{F}_p$, there exist $k+1$ primitive elements $\alpha_1, \alpha_2, \cdots, \alpha_k, \beta \in \mathbb{F}_p$ such that all equations

$$\alpha_1 + \beta = c_1,\ \alpha_2 + \beta = c_2,\ \cdots,\ \alpha_k + \beta = c_k \text{ hold.}$$

Theorem 2 proves a more general and stronger result. That is, if p is a prime large enough and k is any fixed positive integer, then for any k different integers $c_1,\ c_2, \cdots, c_k \in \{1, 2, 3, \cdots, p-1\}$, there exist k primitive roots $\alpha_1, \alpha_2, \cdots, \alpha_k$ and a square-free primitive root β modulo p such that all congruence equations

$$\alpha_1 + \beta \equiv c_1 \bmod p,\ \alpha_2 + \beta \equiv c_2 \bmod p,\ \cdots,\ \alpha_k + \beta \equiv c_k \bmod p \text{ hold.}$$

Of course, Theorem 1 and Theorem 2 are also correct in the finite field $\mathbb{F}_q$.

These results not only solved an open problem ($k = 3$) proposed by W. P. Zhang and T. T. Wang in [3], but also obtained more general conclusions.

Acknowledgments

The authors would like to thank the referee for their very helpful and detailed comments. The authors also express their heartfelt thanks to their supervisor professor Wenpeng Zhang for his very helpful suggestion.

This work is supported by the N. S. F. (11771351) and the Natural Science Basic Research Project in Shaanxi Province (2017JK1002) of P. R. China.

Conflict of interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. S. W. Golomb, *Algebraic constructions for costas arrays*, Journal of Combinatoral Theory Series A, **37** (1984), 13–21.
2. Q. Sun, *On primitive roots in a finite field*, Journal of Sichuan University, Natural Science Edition, **25** (1988), 133–139.
3. W. P. Zhang and T. T. Wang, *The primitive roots and a problem related to the Golomb conjecture*, AIMS Mathematics, **5** (2020), 3899–3905.
4. C. Cobeli and A. Zaharescu, *On the distribution of primitive roots (* mod *p)*, Acta Arith., **83** (1998), 143–153.
5. J. P. Wang, *On Golomb's conjecture*, Science in China (Ser. A.), **9** (1987), 927–935.
6. T. T. Wang and X. N. Wang, *On the Golomb's conjecture and Lehmer's numbers*, Open Math., **15** (2017), 1003–1009.
7. M. Munsch, T. Trudgian, *Square-full primitive roots*, Int. J. Number Theory, **14** (2018), 1013–1021.
8. W. Q. Wang and W. P. Zhang, *A mean value related to primitive roots and Golomb's conjectures*, Absract and Applied analysis, **2014** (2014), 908273.
9. W. P. Zhang, *On a problem related to Golomb's conjectures*, J. Syst. Sci. Complexity, **16** (2003), 13–18.
10. T. Tian and W. Qi, *Primitive normal element and its inverse in finite fields*, Acta Math. Sinica, **49** (2006), 657–668.
11. S. Andrea, *Least primitive root and simultaneous power non-residues*, J. Number Theory, **204** (2019), 246–263.
12. M. Anwar and F. Pappalardi, *On simultaneous primitive roots*, Acta Arith., **180** (2017), 35–43.
13. S. D. Cohen and T. Trudgian, *Lehmer numbers and primitive roots modulo a prime*, J. Number Theory, **203** (2019), 68–79.
14. S. D. Cohen and T. Trudgian, *On the least square-free primitive root modulo p*, J. Number Theory, **170** (2017), 10–16.
15. S. D. Cohen and W. P. Zhang, *Sums of two exact powers*, Finite Fields Th. App., **8** (2002), 471–477.
16. S. D. Cohen, *Pairs of primitive roots*, Mathematica, **32** (1985), 276–285.
17. T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.
18. W. Narkiewicz, *Classical Problems in Number Theory*, Polish Scientifc Publishers, 1986.
19. J. Bourgain, Z. M. Garaev and V. S. Konyagin, *On the hidden shifted power problem*, SIAM J. Comput., **41** (2012), 1524–1557.
20. A. Weil, *Basic number theory*, Springer-Verlag, New York, 1974.
21. L. Carlitz, Sets of primitive roots, *Compos. Math.*, **13** (1956), 65–70.

AIMS Press