Electronic Research Archive

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

ERA, 31(11): 6913–6927.
DOI: 10.3934/era.2023350
Received: 20 April 2023
Revised: 17 September 2023
Accepted: 19 September 2023
Published: 27 October 2023

*Research article*

# On the distribution of primitive roots and Lehmer numbers

**Jiafan Zhang***

Research Center for Number Theory and Its Applications, Northwest University, Xi'an 710127, Shaanxi, China

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

**Abstract:** In this paper, we study the number of the Lehmer primitive roots solutions of a multivariate linear equation and the number of $1 \le x \le p-1$ such that for $f(x) \in \mathbb{F}_p[x]$, $k$ polynomials $f(x+c_1), f(x+c_2), \dots, f(x+c_k)$ are Lehmer primitive roots modulo prime $p$, and obtain asymptotic formulae for these utilizing the properties of Gauss sums and the generalized Kloosterman sums.

**Keywords:** primitive roots; Lehmer numbers; Golomb's conjecture; Gauss sums; the generalized Kloosterman sums

## 1. Introduction

Let $q$ be a power of odd prime. Several researchers have looked into a variety of properties about the primitive roots modulo $q$. Let $g_1, g_2$ represent two primitive roots modulo $q$, $a$, $b$ and $c$ represent arbitrary non-zero elements in $\mathbb{F}_q$. Is there some $q_0$ such that for all $q > q_0$, there is always one representation

$$a = bg_1 + cg_2\ ? \tag{1.1}$$

For $b = 1$ and $c = -1$, Vegh [1] considered a specific form of Eq (1.1), which is known as Vegh's Conjecture, (see [2, §F9 ] for further details). Cohen [3] demonstrated Vegh's Conjecture for all $q > 7$.

For $b = 1$ and $c = 1$, Golomb [4] proposed another specific form of Eq (1.1). This was proved by Sun [5] for $q > 2^{60} \approx 1.15 \times 10^{18}$.

Moreover, Cohen et al. [6] studied linear sums of primitive roots and their inverses in finite fields $\mathbb{F}_q$ and showed that if $q > 13$, then for arbitrary non-zero $a, b \in \mathbb{F}_q$, there is a pair of primitive elements $(g_1, g_2)$ of $\mathbb{F}_q$ such that both $ag_1 + bg_2$ and $ag_1^{-1} + bg_2^{-1}$ are primitive.

Let $p$ be an odd prime. Carlitz [7] relied on some results of Davenport and obtained for any $k-1$ fixed integers $c_1, c_2, \dots, c_{k-1}$ with $c_i \ge 1 (i = 1, 2, \dots, k-1)$. Let $g, g_1, \dots, g_{k-1}$ be primitive roots modulo $p$ and $N_k$ denote the number of $g$ mod $p$ such that $g_1 - g = c_1, \dots, g_{k-1} - g = c_{k-1}$. Then

$$N_k \sim \frac{\phi^k(p-1)}{p^{k-1}} \ (p \to \infty).$$

More results of the primitive roots distribution can be found in [8–11].

Lehmer [2, §F12] proposed the definition of *Lehmer number*, according to which $a$ is a *Lehmer number* if and only if $a$ and $\bar{a}$ have opposite parity, i.e., $(2, a+\bar{a}) = 1$, where $\bar{a}$ is the multiplicative inverse of $a$ modulo $p$. It is simple to demonstrate that there are no Lehmer numbers modulo $p$ when $p = 3$ or 7. Zhang [12] established that if $M_p$ denotes the number of Lehmer numbers modulo $p$, then

$$M_p = \frac{p-1}{2} + \mathrm{O}\left(p^{\frac{1}{2}} \ln^2 p\right).$$

A Lehmer number that is also a primitive root modulo $p$ will be called a *Lehmer primitive root* or an *LPR*. The inverse of an *LPR* is also an *LPR*. We assume that $p > 3$ because there is no Lehmer number modulo 3. Wang and Wang [13] investigated the distribution of *LPRs* involving Golomb's conjecture. Let $G_p$ denote the number of Golomb pairs $(a, b)$ (i.e., $a + b \equiv 1(\bmod p)$) are *LPRs*. They showed

$$G_p = \frac{1}{4}\frac{\phi^2(p-1)}{p-1} + O\left(\frac{\phi^2(p-1)}{p^{\frac{5}{4}}} \cdot 4^{\omega(p-1)} \cdot \ln^2 p\right).$$

Let $N_p$ denote the number of *LPRs* modulo $p$. For odd integers $m \geq 3$, define the positive number $T_m$ by

$$T_m = \frac{2}{m \ln m} \sum_{j=1}^{(m-1)/2} \tan\left(\frac{\pi j}{m}\right).$$

Cohen and Trudgian [14] improved the result of Wang and Wang [13] and showed

$$\left|N_p - \frac{\phi(p-1)}{2}\right| < T_p^2 \frac{\phi(p-1)}{p-1} 2^{\omega(p-1)} p^{\frac{1}{2}} \ln^2 p$$

and

$$\left|G_p - \frac{\phi^2(p-1)}{4(p-1)^2}(p-2)\right| < \frac{\phi^2(p-1)}{4(p-1)^2} T_p^2 [2^{2\omega(p-1)}(9\ln^2 p + 1) - 1] p^{\frac{1}{2}},$$

where $\frac{2}{\pi}\left(1 + \frac{0.548}{\ln p}\right) < T_p < \frac{2}{\pi}\left(1 + \frac{1.549}{\ln p}\right)$.
Specifically, they obtained that for an odd prime $p (\neq 3, 7)$, there exists an *LPR* modulo $p$.

Inspired by the results of Cohen and Trudgian [14] and Wang and Wang [13], we mainly studied the distribution of *LPRs* modulo $p$ related to the Golomb's conjecture in two aspects. On the one hand, we extend Eq (1.1) to the case involving $k > 1$ variables. Let $\mathcal{R}$ be set of *LPRs* modulo $p$ that is a subset of $\mathbb{F}_p$. $a_1, a_2, \dots, a_k, c$ are non-zero elements in $\mathbb{F}_p$ and $N(\mathcal{R}, p)$ denotes the number of solutions of the equation

$$a_1 g_1 + a_2 g_2 + \cdots + a_k g_k = c, \ g_1, g_2, \dots, g_k \in \mathcal{R}.$$

We consider the distribution properties of $N(\mathcal{R}, p)$, and obtain the following:

**Theorem 1.** *Let $p > 3$ be an odd prime. Then we have*

$$N(\mathcal{R}, p) = \frac{\phi^k(p-1)}{2^k p} + \mathrm{O}\left(\frac{\phi^k(p-1)}{p^{\frac{3}{2}}} 2^{k\omega(p-1)} \ln^{2k} p\right),$$

*where the symbol* O *is dependent on k.*

When $k = 2$, we can obtain the number of the Golomb pairs that are *LPRs*.

On the other hand, we consider the distribution of $k$ consecutive *LPRs* and generalize it to a more general form.

Let $f(x) \in \mathbb{F}_p[x]$. Define

$$M(f(x), \mathcal{R}, p) = \#\{x : 1 \le x \le p-1, f(x+c_1), f(x+c_2), \cdots, f(x+c_k) \in \mathcal{R}\}.$$

Then we have:

**Theorem 2.** *Let $f(x) \in \mathbb{F}_p[x]$ with degree $l \ge 1$. $c_1, c_2, \ldots, c_k$ are distinct elements in $\mathbb{F}_p$. Suppose that one of the following conditions holds:*

(i) *$f(x)$ is irreducible,*

(ii) *$f(x)$ has no multiple zero in $\bar{\mathbb{F}}_p$ and $k = 2$,*

(iii) *$f(x)$ has no multiple zero in $\bar{\mathbb{F}}_p$ and $(4k)^l < p$.*

*Then we have*

$$M(f(x), \mathcal{R}, p) = \frac{1}{2^k} \frac{\phi^k(p-1)}{(p-1)^{k-1}} + \mathrm{O}\left(\frac{\phi^k(p-1)}{p^{k-\frac{1}{2}}} 2^{k\omega(p-1)} \ln^{2k} p\right),$$

*where the symbol* O *is dependent on k and l.*

Take $f(x) = x$, $c_k = 0$ in Theorem 2. Then we can get the number of $k$ consecutive primitive roots $x, x + c_1, \ldots, x + c_{k-1}$ are Lehmer numbers, which is:

**Corollary 1.** *Let p be an odd prime. Then for any $1 \le\ x \le (p-1)$ that is an LPR modulo p, we have*

$$M(x, \mathcal{R}, p) = \frac{1}{2^k} \frac{\phi^k(p-1)}{(p-1)^{k-1}} + \mathrm{O}\left(\frac{\phi^k(p-1)}{p^{k-\frac{1}{2}}} 2^{k\omega(p-1)} \ln^{2k} p\right),$$

*where the symbol* O *is dependent on k.*

When $k = 1, 2$, we can easily deduce the Theorem 1 and Theorem 6 in Cohen and Trudgian [14], respectively.

**Notation:** Throughout this paper, $\mathbb{F}_q$ denotes a finite field of characteristic $p$, $\bar{\mathbb{F}}_q$ denotes the algebraic closure of $\mathbb{F}_q$, $\phi(n)$ is reserved for the Euler function, $\mu(n)$ is the Möbius function. We use $\omega(n)$ to denote the number of all distinct prime divisors of $n$. Write $\sum_{\chi_d}$ to denote a sum over all $\phi(d)$ multiplicative characters $\chi_d$ of order $d$ over $\mathbb{F}_p$, and denote by ${\sum_{n=1}^{p}}'$ the summation of $1 \le n \le p$ with $(n, p) = 1$. $\tau(\chi)$ is the classical Gauss sums associated with character $\chi$ mudulo $p$. $f \ll g$ means $|f| \le cg$ with some positive constant $c$, $f = \mathrm{O}(g)$ means $f \ll g$.

## 2. Some lemmas

To complete the proof of the theorems, we need following several lemmas. The proofs of these lemmas require some basic knowledge of analytic number theory, which can be found in [15].

**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*

$$\frac{\phi(p-1)}{p-1}\sum_{d|p-1}\frac{\mu(d)}{\phi(d)}\sum_{\chi_d}\chi_d(a)=\begin{cases}1, & \textit{if } a \textit{ is a primitive root} \bmod p;\\ 0, & \textit{if } a \textit{ is not a primitive root} \bmod p.\end{cases}$$

*Proof.* See Proposition 2.2 of Narkiewicz [16]. □

**Lemma 2.** *Let $p$ be an odd prime, $\chi$ be a nonprincipal multiplicative character modulo $p$ of order $d$. Suppose $g(x)\in\mathbb{F}_p[x]$ has precisely $m$ distinct ones among its zeros, and suppose that $g(x)$ is not the constant multiple of a $d$-th power over $\mathbb{F}_q$. Then*

$$\left|\sum_{x\in\mathbb{F}_p}\chi\left(g(x)\right)\right|\le(m-1)\cdot p^{\frac{1}{2}}.$$

*Proof.* See Theorem 2C in Chapter 2 of Schmidt [17]. □

**Lemma 3.** *Let $\mathbb{F}_q$ be a finite field of characteristic $p$, $\psi$ be a nontrivial additive character and $\chi$ be a nonprincipal multiplicative character on $\mathbb{F}_q$ of order $d$. For two rational functions $f(x), g(x)\in\mathbb{F}_q[x]$, define $K(\psi,f;\chi,g)=\sum_{x\in\mathbb{F}_q\setminus S}\chi(g(x))\psi(f(x))$, where $S$ denotes the set of poles of $f(x)$ and $g(x)$. Suppose the following conditions hold:*

(i) *$g(x)$ is not the constant multiple of a $d$-th power over $\mathbb{F}_q$.*

(ii) *$f(x)$ is not of the form $(h(x))^p-h(x)$ with a rational function $h(x)$ over $\mathbb{F}_q$.*

*Then we have*

$$|K(\psi,f;\chi,g)|\le(\deg(f)+m-1)\sqrt{q},$$

*where $m$ is the number of distinct roots and (noninfinite) poles of $g(x)$ in $\mathbb{F}_q$.*

*Proof.* See Theorem 2G in Chapter 2 of Schmidt [17]. □

**Lemma 4.** *Let $p$ be an odd prime. Let $c_1,\cdots,c_k$ be distinct elements in $\mathbb{F}_p$. Assume that $f(x)\in\mathbb{F}_p[x]$ with $\deg(f)=l$. Define the polynomial*

$$h(x)=f(x+c_1)\cdots f(x+c_k).$$

*Suppose one of the following conditions holds:*

(i) *$f(x)$ is irreducible,*

(ii) *$f(x)$ has no multiple zero in $\bar{\mathbb{F}}_p$ and $k=2$,*

(iii) *$f(x)$ has no multiple zero in $\bar{\mathbb{F}}_p$ and $(4k)^l<p$.*

*Then $h(x)$ has at least one simple root in $\bar{\mathbb{F}}_p$.*

*Proof.* Suppose that $f(x)$ is irreducible. Then $f(x+c_1),\cdots,f(x+c_k)$ are distinct irreducible polynomials, and $h(x)$ has at least $k$ simple roots in $\bar{\mathbb{F}}_p$. The cases of (ii) and (iii) can be proved by Theorem 2 and Lemma 2 of [18], for $k=2$ or $(4k)^l<p$, $(l,k,p)$ is "admissible triple," then $f(x+c_1)\cdots f(x+c_k)$ has at least one simple root. □

**Lemma 5.** *Let p be an odd prime, $m_1,\dots,m_k,n_1,\dots,n_k$ be integers with $(m_1\cdots m_k n_1\cdots n_k,p)=1$, and polynomials $g(x),f_1(x),\dots,f_k(x)\in\mathbb{F}_p[x]$. Let $\chi$ be a Dirichlet character modulo p of order d. Define*

$$K(\chi,g,f_1,\cdots,f_k;p)$$
$$=\sum_{\substack{x=1\\(f_1(x)\cdots f_k(x),p)=1}}^{p}\chi(g(x))e\left(\frac{m_1f_1(x)+\cdots+m_kf_k(x)+n_1\overline{f_1(x)}+\cdots+n_k\overline{f_k(x)}}{p}\right).$$

*Suppose the following conditions hold:*

(i) *$g(x)$ can not be the constant multiple of a d-th power over $\mathbb{F}_p$.*

(ii) *$F(x)=f_1(x)\cdots f_k(x)$ has at least one simple root in $\bar{\mathbb{F}}_p$.*

*Then we have*

$$|K(\chi,g,f_1,\cdots,f_k;p)|\le(\max(\deg(f_1),\cdots,\deg(f_k))+l)\sqrt{p},$$

*where $e(x)=e^{2\pi ix}$ and l is the number of distinct roots of $g(x)$ in $\bar{\mathbb{F}}_p$.*

*Proof.* It is clear that

$$m_1f_1(x)+\cdots+m_kf_k(x)+n_1\overline{f_1(x)}+\cdots+n_k\overline{f_k(x)}$$
$$=\frac{F(x)(m_1f_1(x)+\cdots+m_kf_k(x))+n_1\frac{F(x)}{f_1(x)}+\cdots+n_k\frac{F(x)}{f_k(x)}}{F(x)}:=\frac{G(x)}{F(x)}.$$

Condition (i) is the same as Lemma 3. So our goal is to prove the rational function $G(x)/F(x)$ satisfies condition (ii) in Lemma 3 if $F(x)$ has a simple root in $\bar{\mathbb{F}}_p$. Assume that there are polynomials $K(x),L(x)\in\mathbb{F}_p[x]$ with $(K(x),L(x))=1$ such that

$$\frac{G(x)}{F(x)}=\left(\frac{K(x)}{L(x)}\right)^p-\left(\frac{K(x)}{L(x)}\right).$$

Then we have

$$G(x)L(x)^p=\left(K(x)^p-K(x)L(x)^{p-1}\right)F(x). \tag{2.1}$$

Since $F(x)=f_1(x)\cdots f_k(x)$ has at least one simple root in $\bar{\mathbb{F}}_p$, then there exists an irreducible polynomial $w(x)\in\mathbb{F}_p[x]$ such that $w(x)\mid F(x)$ and $w(x)^2\nmid F(x)$. Assume that $w(x)\mid f_1(x)$, then we have

$$w(x)\nmid\frac{F(x)}{f_1(x)},\ w(x)\mid\frac{F(x)}{f_i(x)}(i=2,\cdots,k).$$

Hence, from Eq (2.1)

$$w(x)\nmid G(x)\Longrightarrow w(x)\mid L(x)^p\Longrightarrow w(x)\mid L(x)$$

$$w(x)^2 \mid L(x)^{p-1} \Longrightarrow w(x)^2 \mid K(x)^p F(x) \Longrightarrow w(x) \mid K(x),$$

which contradicts to $(K(x), L(x)) = 1$. Therefore, from Lemma 3 we get

$$|K(\chi, g, f_1, \cdots, f_k; p)| \le (\max(\deg(f_1), \cdots, \deg(f_k)) + l)\ \sqrt{p},$$

where $l$ is the number of distinct roots of $g(x)$ in $\bar{\mathbb{F}}_p$. □

**Lemma 6.** *Let $\chi$ be a primitive character modulo $p$, $\chi_{d_i}$ be character modulo $p$ of order $d_i$. There exist some $1 \le s_i \le d_i$ with $(s_i, d_i) = 1$, $i = 1, 2, \ldots, k$. Then we have*

$$\begin{aligned}&\sum_{\chi_{d_1}} \cdots \sum_{\chi_{d_k}} \chi_{d_1}(f(x+c_1)) \cdots \chi_{d_k}(f(x+c_k))\\ =\ &\sum_{s_1=1}^{d_1}{}' \cdots \sum_{s_k=1}^{d_k}{}' \chi\left((f(x+c_1))^{\frac{s_1(p-1)}{d_1}} \cdots (f(x+c_k))^{\frac{s_k(p-1)}{d_k}}\right).\end{aligned}$$

*Proof.* From the definition of the Dirichlet character modulo $p$, we can get

$$\begin{aligned}&\sum_{\chi_{d_1}} \cdots \sum_{\chi_{d_k}} \chi_{d_1}(f(x+c_1)) \cdots \chi_{d_k}(f(x+c_k))\\ =\ &\sum_{s_1=1}^{d_1}{}' \cdots \sum_{s_k=1}^{d_k}{}' e\left(\frac{s_1 \cdot \mathrm{ind}(f(x+c_1))}{d_1}\right) \cdots e\left(\frac{s_k \cdot \mathrm{ind}(f(x+c_k))}{d_k}\right)\\ =\ &\sum_{s_1=1}^{d_1}{}' \cdots \sum_{s_k=1}^{d_k}{}' e\left(\frac{\frac{s_1(p-1)}{d_1} \cdot \mathrm{ind}(f(x+c_1)) + \cdots + \frac{s_k(p-1)}{d_k} \cdot \mathrm{ind}(f(x+c_k))}{p-1}\right)\\ =\ &\sum_{s_1=1}^{d_1}{}' \cdots \sum_{s_k=1}^{d_k}{}' e\left(\frac{\mathrm{ind}(f(x+c_1))^{\frac{s_1(p-1)}{d_1}} + \cdots + \mathrm{ind}(f(x+c_k))^{\frac{s_k(p-1)}{d_k}}}{p-1}\right)\\ =\ &\sum_{s_1=1}^{d_1}{}' \cdots \sum_{s_k=1}^{d_k}{}' e\left(\frac{\mathrm{ind}\left((f(x+c_1))^{\frac{s_1(p-1)}{d_1}} \cdots (f(x+c_k))^{\frac{s_k(p-1)}{d_k}}\right)}{p-1}\right)\\ =\ &\sum_{s_1=1}^{d_1}{}' \cdots \sum_{s_k=1}^{d_k}{}' \chi\left(f(x+c_1))^{\frac{s_1(p-1)}{d_1}} \cdots (f(x+c_k))^{\frac{s_k(p-1)}{d_k}}\right),\end{aligned}$$

where ind($a$) denotes an index of $a$ with base $g$ of modulo $p$, and $g$ is a positive primitive root of modulo $p$. □

## 3. Proofs of the theorems

Firstly, we prove the Theorem 1. Let $p$ be an odd prime, $k$ be any fixed positive integer. Then for any $k$ different integers $a_1,\ a_2, \ldots, a_k \in \mathbb{F}_p$, from Lemma 1 and the definition of Lehmer number we have

$$N(\mathcal{R}, p) = \frac{1}{p} \sum_{b=0}^{p-1} \sum_{g_1=1}^{p-1} \sum_{g_2=1}^{p-1} \cdots \sum_{\substack{g_k=1\\ g_1,g_2,\ldots,g_k \in \mathcal{R}}}^{p-1} e\left(\frac{b(a_1 g_1 + \cdots + a_k g_k - c)}{p}\right)$$

$$
\begin{aligned}
&= \frac{1}{p}\frac{\phi^k(p-1)}{2^k(p-1)^k}\prod_{i=1}^{k}\left(\sum_{d_i|p-1}\frac{\mu(d_i)}{\phi(d_i)}\sum_{\chi_{d_i}}\sum_{g_i=1}^{p-1}\chi_{d_i}(g_i)\left(1-(-1)^{g_i+\overline{g_i}}\right)\right)\\
&\quad\cdot\sum_{b=0}^{p-1} e\left(\frac{b(a_1g_1+\cdots+a_kg_k-c)}{p}\right)\\
&= \frac{1}{p}\frac{\phi^k(p-1)}{2^k(p-1)^k}\prod_{i=1}^{k}\left(\sum_{d_i|p-1}\frac{\mu(d_i)}{\phi(d_i)}\sum_{\chi_{d_i}}\sum_{g_i=1}^{p-1}\chi_{d_i}(g_i)\right)\sum_{b=0}^{p-1} e\left(\frac{b(a_1g_1+\cdots+a_kg_k-c)}{p}\right)\\
&\quad+\frac{1}{p}\frac{\phi^k(p-1)}{2^k(p-1)^k}\prod_{i=1}^{k}\left(\sum_{d_i|p-1}\frac{\mu(d_i)}{\phi(d_i)}\sum_{\chi_{d_i}}\sum_{g_i=1}^{p-1}\chi_{d_i}(g_i)\right)\sum_{t=1}^{k}(-1)^t\sum_{i_1=1}^{k}\sum_{\substack{i_2=1\\ i_1<i_2<\cdots<i_t}}^{k}\cdots\sum_{i_t=1}^{k} l_{i_1}l_{i_2}\cdots l_{i_t}\\
&\quad\cdot\sum_{b=0}^{p-1} e\left(\frac{b(a_1g_1+\cdots+a_kg_k-c)}{p}\right)\\
&= A_1+A_2, \qquad (3.1)
\end{aligned}
$$

where $l_i=(-1)^{g_i+\overline{g_i}}, i=1,2,\cdots,k.$

$$
\begin{aligned}
A_1 &= \frac{1}{p}\frac{\phi^k(p-1)}{2^k(p-1)^k}\prod_{i=1}^{k}\left(\sum_{d_i|p-1}\frac{\mu(d_i)}{\phi(d_i)}\sum_{\chi_{d_i}}\sum_{g_i=1}^{p-1}\chi_{d_i}(g_i)\right)\sum_{b=0}^{p-1} e\left(\frac{b(a_1g_1+\cdots+a_kg_k-c)}{p}\right)\\
&= \frac{1}{p}\frac{\phi^k(p-1)}{2^k(p-1)^k}\left[\sum_{g_1=1}^{p-1}\cdots\sum_{g_k=1}^{p-1}\sum_{b=0}^{p-1} e\left(\frac{b(a_1g_1+\cdots+a_kg_k-c)}{p}\right)\right.\\
&\quad+\sum_{d_1|p-1}\underset{d_1\cdots d_k>1}{\cdots}\sum_{d_k|p-1}\frac{\mu(d_1)}{\phi(d_1)}\cdots\frac{\mu(d_k)}{\phi(d_k)}\sum_{\chi_{d_1}}\cdots\sum_{\chi_{d_k}}\sum_{g_1=1}^{p-1}\cdots\sum_{g_k=1}^{p-1}\chi_{d_1}(g_1)\cdots\chi_{d_k}(g_k)\\
&\quad\left.\cdot\sum_{b=0}^{p-1} e\left(\frac{b(a_1g_1+\cdots+a_kg_k-c)}{p}\right)\right]\\
&= \frac{1}{p}\frac{\phi^k(p-1)}{2^k(p-1)^k}\left[(p-1)^k+(-1)^{k+1}+\sum_{d_1|p-1}\underset{d_1\cdots d_k>1}{\cdots}\sum_{d_k|p-1}\frac{\mu(d_1)}{\phi(d_1)}\cdots\frac{\mu(d_k)}{\phi(d_k)}\right.\\
&\quad\left.\cdot\sum_{\chi_{d_1}}\cdots\sum_{\chi_{d_k}}\sum_{g_1=1}^{p-1}\cdots\sum_{g_k=1}^{p-1}\chi_{d_1}(g_1)\cdots\chi_{d_k}(g_k)\sum_{b=0}^{p-1} e\left(\frac{b(a_1g_1+\cdots+a_kg_k-c)}{p}\right)\right]. \qquad (3.2)
\end{aligned}
$$

From Eq (3.2), let

$$
\begin{aligned}
A_{11} &= \sum_{d_1|p-1}\underset{d_1\cdots d_k>1}{\cdots}\sum_{d_k|p-1}\frac{\mu(d_1)}{\phi(d_1)}\cdots\frac{\mu(d_k)}{\phi(d_k)}\sum_{\chi_{d_1}}\cdots\sum_{\chi_{d_k}}\sum_{g_1=1}^{p-1}\cdots\sum_{g_k=1}^{p-1}\chi_{d_1}(g_1)\cdots\chi_{d_k}(g_k)\\
&\quad\cdot\sum_{b=0}^{p-1} e\left(\frac{b(a_1g_1+a_2g_2+\cdots+a_kg_k-c)}{p}\right)
\end{aligned}
$$

$$= \sum_{\substack{d_1|p-1 \\ d_1\cdots d_k>1}} \cdots \sum_{d_k|p-1} \frac{\mu(d_1)}{\phi(d_1)} \cdots \frac{\mu(d_k)}{\phi(d_k)} \sum_{\chi_{d_1}} \cdots \sum_{\chi_{d_k}} \sum_{g_1=1}^{p-1} \cdots \sum_{g_k=1}^{p-1} \chi_{d_1}(g_1) \cdots \chi_{d_k}(g_k)$$

$$+ \sum_{\substack{d_1|p-1 \\ d_1\cdots d_k>1}} \cdots \sum_{d_k|p-1} \frac{\mu(d_1)}{\phi(d_1)} \cdots \frac{\mu(d_k)}{\phi(d_k)} \sum_{\chi_{d_1}} \cdots \sum_{\chi_{d_k}} \sum_{b=1}^{p-1} \sum_{g_1=1}^{p-1} \chi_{d_1}(g_1) e\left(\frac{ba_1g_1}{p}\right)$$

$$\cdots \sum_{g_k=1}^{p-1} \chi_{d_k}(g_k) e\left(\frac{ba_kg_k}{p}\right) e\left(\frac{-bc}{p}\right)$$

$$= \sum_{\substack{d_1|p-1 \\ d_1\cdots d_k>1}} \cdots \sum_{d_k|p-1} \frac{\mu(d_1)}{\phi(d_1)} \cdots \frac{\mu(d_k)}{\phi(d_k)} \sum_{\chi_{d_1}} \cdots \sum_{\chi_{d_k}} \sum_{b=1}^{p-1} \sum_{g_1=1}^{p-1} \chi_{d_1}(g_1) e\left(\frac{ba_1g_1}{p}\right)$$

$$\cdots \sum_{g_k=1}^{p-1} \chi_{d_k}(g_k) e\left(\frac{ba_kg_k}{p}\right) e\left(\frac{-bc}{p}\right).$$

Using the properties of Gauss sums we can get

$$|A_{11}| = \Bigg| \sum_{\substack{d_1|p-1 \\ d_1\cdots d_k>1}} \cdots \sum_{d_k|p-1} \frac{\mu(d_1)}{\phi(d_1)} \cdots \frac{\mu(d_k)}{\phi(d_k)} \sum_{\chi_{d_1}} \cdots \sum_{\chi_{d_k}} \sum_{b=1}^{p-1} \sum_{g_1=1}^{p-1} \chi_{d_1}(g_1) e\left(\frac{ba_1g_1}{p}\right)$$

$$\cdots \sum_{g_k=1}^{p-1} \chi_{d_k}(g_k) e\left(\frac{ba_kg_k}{p}\right) e\left(\frac{-bc}{p}\right) \Bigg|$$

$$= \Bigg| \sum_{\substack{d_1|p-1 \\ d_1>1}} \cdots \sum_{\substack{d_k|p-1 \\ d_k>1}} \frac{\mu(d_1)}{\phi(d_1)} \cdots \frac{\mu(d_k)}{\phi(d_k)} \sum_{\chi_{d_1}} \cdots \sum_{\chi_{d_k}} \sum_{b=1}^{p-1} \sum_{g_1=1}^{p-1} \chi_{d_1}(g_1) e\left(\frac{ba_1g_1}{p}\right)$$

$$\cdots \sum_{g_k=1}^{p-1} \chi_{d_k}(g_k) e\left(\frac{ba_kg_k}{p}\right) e\left(\frac{-bc}{p}\right)$$

$$+ \sum_{\substack{d_1|p-1 \\ d_1>1}} \cdots \sum_{\substack{d_{k-1}|p-1 \\ d_{k-1}>1}} \frac{\mu(d_1)}{\phi(d_1)} \cdots \frac{\mu(d_{k-1})}{\phi(d_{k-1})} \sum_{\chi_{d_1}} \cdots \sum_{\chi_{d_{k-1}}} \sum_{b=1}^{p-1} \sum_{g_1=1}^{p-1} \chi_{d_1}(g_1) e\left(\frac{ba_1g_1}{p}\right)$$

$$\cdots \sum_{g_{k-1}=1}^{p-1} \chi_{d_{k-1}}(g_{k-1}) e\left(\frac{ba_{k-1}g_{k-1}}{p}\right) \sum_{g_k=1}^{p-1} e\left(\frac{ba_kg_k}{p}\right) e\left(\frac{-bc}{p}\right)$$

$$+ \cdots + \sum_{\substack{d_1|p-1 \\ d_1>1}} \frac{\mu(d_1)}{\phi(d_1)} \sum_{\chi_{d_1}} \sum_{b=1}^{p-1} \sum_{g_1=1}^{p-1} \chi_{d_1}(g_1) e\left(\frac{ba_1g_1}{p}\right) \sum_{g_2=1}^{p-1} e\left(\frac{ba_2g_2}{p}\right)$$

$$\cdots \sum_{g_k=1}^{p-1} e\left(\frac{ba_kg_k}{p}\right) e\left(\frac{-bc}{p}\right) \Bigg|$$

$$\ll \quad 2^{k\omega(p-1)}p^{\frac{k+1}{2}},$$

where we have used the fact that $\sum_{d|n}|\mu(d)| = 2^{\omega(n)}$.

Hence, Eq (3.2) and the above formulae yield that

$$A_1 = \frac{\phi^k(p-1)}{2^k p} + \mathrm{O}\left(\frac{\phi^k(p-1)}{p^{\frac{k+1}{2}}}2^{k\omega(p-1)}\right). \tag{3.3}$$

Then we compute $A_2$ in Eq (3.1). For simplicity, let

$$U_m(u) = \sum_{u=1}^{p-1}(-1)^u e\left(\frac{-mu}{p}\right),$$

noting that

$$\sum_{u=1}^{p-1}(-1)^u e\left(\frac{-mu}{p}\right) = \frac{1-e(\frac{m}{p})}{1+e(\frac{m}{p})} = \frac{i\sin(\pi m/p)}{\cos(\pi m/p)},$$

$$\sum_{m=1}^{p-1}\left|\frac{\sin(\pi m/p)}{\cos(\pi m/p)}\right| = T_p p\ln p.$$

Hence,

$$\left|\sum_{m=1}^{p-1}U_m(u)\right| \le \sum_{m=1}^{p-1}\left|\sum_{u=1}^{p-1}(-1)^u e\left(\frac{-mu}{p}\right)\right| = T_p p\ln p. \tag{3.4}$$

Noting that, if $m=0$, then $\sum_{u=1}^{p-1}(-1)^u e\left(\frac{-mu}{p}\right) = \sum_{u=1}^{p-1}(-1)^u = 0$, since $p$ is odd. Hence,

$$\begin{aligned}
& l_i = (-1)^{g_i+\overline{g_i}} \\
= \ & \frac{1}{p}\sum_{m_i=0}^{p-1}\sum_{u_i=1}^{p-1}(-1)^{u_i}e\left(\frac{m_i(g_i-u_i)}{p}\right)\cdot\frac{1}{p}\sum_{n_i=0}^{p-1}\sum_{v_i=1}^{p-1}(-1)^{v_i}e\left(\frac{n_i(\overline{g_i}-v_i)}{p}\right) \\
= \ & \frac{1}{p^2}\sum_{m_i,n_i=0}^{p-1}e\left(\frac{m_ig_i+n_i\overline{g_i}}{p}\right)\sum_{u_i=1}^{p-1}(-1)^{u_i}e\left(\frac{-m_iu_i}{p}\right)\sum_{v_i=1}^{p-1}(-1)^{v_i}e\left(\frac{-n_iv_i}{p}\right) \\
= \ & \frac{1}{p^2}\sum_{m_i,n_i=1}^{p-1}e\left(\frac{m_ig_i+n_i\overline{g_i}}{p}\right)U_{m_i}(u_i)U_{n_i}(v_i).
\end{aligned} \tag{3.5}$$

From the above discussion and Eq (3.1), we can obtain

$$\begin{aligned}
|A_2| \ = \ & \left|\frac{1}{p}\frac{\phi^k(p-1)}{2^k(p-1)^k}\prod_{i=1}^{k}\left(\sum_{d_i|p-1}\frac{\mu(d_i)}{\phi(d_i)}\sum_{\chi_{d_i}}\sum_{g_i=1}^{p-1}\chi_{d_i}(g_i)\right)\sum_{t=1}^{k}(-1)^t\sum_{\substack{i_1=1\\ i_1<\cdots<i_t}}^{k}\cdots\sum_{i_t=1}^{k}l_{i_1}\cdots l_{i_t}\right. \\
& \left.\cdot\sum_{b=0}^{p-1}e\left(\frac{b(a_1g_1+a_2g_2+\cdots+a_kg_k-c)}{p}\right)\right|
\end{aligned}$$

$$
\begin{aligned}
\leq\ & \frac{1}{p}\frac{\phi^k(p-1)}{2^k(p-1)^k}\sum_{t=1}^{k}\binom{k}{t}T_p^{2t}\ln^{2t}p\sum_{d_1|p-1}\cdots\sum_{d_k|p-1}\frac{|\mu(d_1)|}{\phi(d_1)}\cdots\frac{|\mu(d_k)|}{\phi(d_k)}\\
& \sum_{\chi_{d_1}}\cdots\sum_{\chi_{d_k}}\Bigg|\sum_{b=0}^{p-1}\sum_{g_1=1}^{p-1}\cdots\sum_{g_k=1}^{p-1}\chi_{d_1}(g_1)\cdots\chi_{d_k}(g_k)\\
& \cdot e\left(\frac{m_1g_1+n_1\overline{g_1}+\cdots+m_tg_t+n_t\overline{g_t}}{p}\right)e\left(\frac{b(a_1g_1+\cdots+a_kg_k-c)}{p}\right)\Bigg|\\
=\ & \frac{1}{p}\frac{\phi^k(p-1)}{2^k(p-1)^k}\sum_{t=1}^{k}\binom{k}{t}T_p^{2t}\ln^{2t}p\Bigg[\sum_{\substack{d_1|p-1\\ d_1>1}}\cdots\sum_{\substack{d_k|p-1\\ d_k>1}}\frac{|\mu(d_1)|}{\phi(d_1)}\cdots\frac{|\mu(d_k)|}{\phi(d_k)}\\
& \sum_{\chi_{d_1}}\cdots\sum_{\chi_{d_k}}\Bigg|\sum_{b=0}^{p-1}\sum_{g_1=1}^{p-1}\cdots\sum_{g_k=1}^{p-1}\chi_{d_1}(g_1)\cdots\chi_{d_k}(g_k)\\
& \cdot e\left(\frac{m_1g_1+n_1\overline{g_1}+\cdots+m_tg_t+n_t\overline{g_t}}{p}\right)e\left(\frac{b(a_1g_1+\cdots+a_kg_k-c)}{p}\right)\Bigg|\\
& +\sum_{\substack{d_1|p-1\\ d_1>1}}\cdots\sum_{\substack{d_{k-1}|p-1\\ d_{k-1}>1}}\frac{|\mu(d_1)|}{\phi(d_1)}\cdots\frac{|\mu(d_{k-1})|}{\phi(d_{k-1})}\\
& \sum_{\chi_{d_1}}\cdots\sum_{\chi_{d_{k-1}}}\Bigg|\sum_{b=0}^{p-1}\sum_{g_1=1}^{p-1}\cdots\sum_{g_k=1}^{p-1}\chi_{d_1}(g_1)\cdots\chi_{d_{k-1}}(g_{k-1})\\
& \cdot e\left(\frac{m_1g_1+n_1\overline{g_1}+\cdots+m_tg_t+n_t\overline{g_t}}{p}\right)e\left(\frac{b(a_1g_1+\cdots+a_kg_k-c)}{p}\right)\Bigg|\\
& +\cdots+\sum_{\substack{d_1|p-1\\ d_1>1}}\frac{|\mu(d_1)|}{\phi(d_1)}\sum_{\chi_{d_1}}\Bigg|\sum_{b=0}^{p-1}\sum_{g_1=1}^{p-1}\cdots\sum_{g_k=1}^{p-1}\chi_{d_1}(g_1)\\
& \cdot e\left(\frac{m_1g_1+n_1\overline{g_1}+\cdots+m_tg_t+n_t\overline{g_t}}{p}\right)e\left(\frac{b(a_1g_1+\cdots+a_kg_k-c)}{p}\right)\Bigg|\\
& +\Bigg|\sum_{b=0}^{p-1}\sum_{g_1=1}^{p-1}\cdots\sum_{g_k=1}^{p-1}e\left(\frac{m_1g_1+n_1\overline{g_1}+\cdots+m_tg_t+n_t\overline{g_t}}{p}\right)\\
& \cdot e\left(\frac{b(a_1g_1+\cdots+a_kg_k-c)}{p}\right)\Bigg|\Bigg]. \qquad (3.6)
\end{aligned}
$$

Summing the above formula for $t$ from 1 to $k$, then the last term of Eq (3.6) is

$$
\begin{aligned}
& \frac{1}{p}\frac{\phi^k(p-1)}{2^k(p-1)^k}\sum_{t=1}^{k}\binom{k}{t}T_p^{2t}\ln^{2t}p\Bigg|\sum_{b=0}^{p-1}\sum_{g_1=1}^{p-1}\cdots\sum_{g_k=1}^{p-1}e\left(\frac{m_1g_1+n_1\overline{g_1}+\cdots+m_tg_t+n_t\overline{g_t}}{p}\right)\\
& \cdot e\left(\frac{b(a_1g_1+\cdots+a_kg_k-c)}{p}\right)\Bigg|
\end{aligned}
$$

$$\begin{aligned}
&= \frac{1}{p}\frac{\phi^k(p-1)}{2^k(p-1)^k}\Bigg[kT_p^2\ln^2 p\Bigg|\sum_{b=0}^{p-1}\sum_{g_1=1}^{p-1}\cdots\sum_{g_k=1}^{p-1} e\left(\frac{m_1g_1+n_1\overline{g_1}}{p}\right)e\left(\frac{b(a_1g_1+\cdots+a_kg_k-c)}{p}\right)\Bigg| \\
&\quad +\cdots+\binom{k}{k-1}T_p^{2(k-1)}\ln^{2(k-1)}p\cdot\Bigg|\sum_{b=0}^{p-1}\sum_{g_1=1}^{p-1}\cdots\sum_{g_k=1}^{p-1} \\
&\quad \cdot e\left(\frac{m_1g_1+n_1\overline{g_1}+\cdots+m_{k-1}g_{k-1}+n_{k-1}\overline{g_{k-1}}}{p}\right)e\left(\frac{b(a_1g_1+\cdots+a_kg_k-c)}{p}\right)\Bigg| \\
&\quad +T_p^{2k}\ln^{2k}p\Bigg|\sum_{b=0}^{p-1}\sum_{g_1=1}^{p-1}\cdots\sum_{g_k=1}^{p-1} e\left(\frac{m_1g_1+n_1\overline{g_1}+\cdots+m_kg_k+n_k\overline{g_k}}{p}\right) \\
&\quad \cdot e\left(\frac{b(a_1g_1+\cdots+a_kg_k-c)}{p}\right)\Bigg|\Bigg] \\
&\ll \frac{\phi^k(p-1)}{p^{k+1}}\ln^{2k}p\left(p^{k-\frac{1}{2}}+\cdots+p^{\frac{k+1}{2}}\right) \\
&\ll \frac{\phi^k(p-1)}{p^{k+1}}\ln^{2k}p\cdot p^{k-\frac{1}{2}} = \frac{\phi^k(p-1)}{p^{\frac{3}{2}}}\ln^{2k}p,
\end{aligned}$$

here we have utilized $T_p^2 < \frac{4}{\pi^2}\left(1+\frac{1.549}{\ln p}\right)^2 < 2.4$ and the results in Wang and Wang (see Lemma 2.2 of [13]) that

$$\left|\sum_{a=1}^{p-1}\chi_d(a)e\left(\frac{ma+n\overline{a}}{p}\right)\right| \ll p^{\frac{1}{2}}.$$

Similarly, note that $\sum_{d|n}|\mu(d)| = 2^{\omega(n)}$ and we can get the estimate of the other terms of Eq (3.6). Then we have

$$A_2 \ll \frac{\phi^k(p-1)}{p^{\frac{3}{2}}}2^{k\omega(p-1)}\ln^{2k}p. \tag{3.7}$$

Inserting Eqs (3.3) and (3.7) into (3.1), we can deduce that

$$\begin{aligned}
N(\mathcal{R},p) &= \frac{\phi^k(p-1)}{2^kp}+\mathrm{O}\left(\frac{\phi^k(p-1)}{p^{\frac{k+1}{2}}}2^{k\omega(p-1)}\right)+\mathrm{O}\left(\frac{\phi^k(p-1)}{p^{\frac{3}{2}}}2^{k\omega(p-1)}\ln^{2k}p\right) \\
&= \frac{\phi^k(p-1)}{2^kp}+\mathrm{O}\left(\frac{\phi^k(p-1)}{p^{\frac{3}{2}}}2^{k\omega(p-1)}\ln^{2k}p\right).
\end{aligned}$$

This proves the Theorem 1.

Now we prove the Theorem 2. Let $\mathcal{A}$ denote the set of integers $1 \le x \le p$ such that

$$\prod_{i=1}^{k}f(x+c_i) \equiv 0(\mathrm{mod}p).$$

By the definition of primitive roots and Lehmer number, it follows that

$$M(f(x),\mathcal{R},p)$$

$$\begin{aligned}
&= \frac{1}{2^k}\frac{\phi^k(p-1)}{(p-1)^k}\prod_{i=1}^{k}\left(\sum_{d_i|p-1}\frac{\mu(d_i)}{\phi(d_i)}\sum_{\chi_{d_i}}\sum_{\substack{x=1\\ x\notin\mathcal{A}}}^{p}\chi_{d_i}(f(x+c_i))\left(1-(-1)^{f(x+c_i)+\overline{f(x+c_i)}}\right)\right)\\
&= \frac{1}{2^k}\frac{\phi^k(p-1)}{(p-1)^k}\prod_{i=1}^{k}\left(\sum_{d_i|p-1}\frac{\mu(d_i)}{\phi(d_i)}\sum_{\chi_{d_i}}\sum_{\substack{x=1\\ x\notin\mathcal{A}}}^{p}\chi_{d_i}(f(x+c_i))\right)\\
&\quad+\frac{1}{2^k}\frac{\phi^k(p-1)}{(p-1)^k}\prod_{i=1}^{k}\left(\sum_{d_i|p-1}\frac{\mu(d_i)}{\phi(d_i)}\sum_{\chi_{d_i}}\sum_{\substack{x=1\\ x\notin\mathcal{A}}}^{p}\chi_{d_i}(f(x+c_i))\right)\sum_{t=1}^{k}(-1)^t\sum_{i_1=1}^{k}\cdots\sum_{\substack{i_t=1\\ i_1<\cdots<i_t}}^{k}g_{i_1}\cdots g_{i_t}\\
&= \frac{1}{2^k}\frac{\phi^k(p-1)}{(p-1)^k}\left(B_1+B_2\right), \qquad (3.8)
\end{aligned}$$

where $g_i=(-1)^{f(x+c_i)+\overline{f(x+c_i)}}, i=1,2,\ldots,k.$

$$\begin{aligned}
B_1 &= \prod_{i=1}^{k}\left(\sum_{d_i|p-1}\frac{\mu(d_i)}{\phi(d_i)}\sum_{\chi_{d_i}}\sum_{\substack{x=1\\ x\notin\mathcal{A}}}^{p}\chi_{d_i}(f(x+c_i))\right)\\
&= \sum_{\substack{x=1\\ x\notin\mathcal{A}}}^{p}1+\prod_{i=1}^{k}\left(\sum_{\substack{d_i|p-1\\ \prod_{i=1}^{k}d_i>1}}\frac{\mu(d_i)}{\phi(d_i)}\sum_{\chi_{d_i}}\sum_{\substack{x=1\\ x\notin\mathcal{A}}}^{p}\chi_{d_i}(f(x+c_i))\right).
\end{aligned}$$

Obviously,

$$\left|\sum_{\substack{x=1\\ x\notin\mathcal{A}}}^{p}1-p\right|\leq kl.$$

From Lemma 6 we have

$$\begin{aligned}
&\sum_{\chi_{d_1}}\sum_{\chi_{d_2}}\cdots\sum_{\chi_{d_k}}\sum_{\substack{x=1\\ x\notin\mathcal{A}}}^{p}\chi_{d_1}(f(x+c_1))\chi_{d_2}(f(x+c_2))\cdots\chi_{d_k}(f(x+c_k))\\
&= \sum_{s_1=1}^{d_1}{}'\cdots\sum_{s_k=1}^{d_k}{}'\sum_{\substack{x=1\\ x\notin\mathcal{A}}}^{p}\chi\left((f(x+c_1))^{\frac{s_1(p-1)}{d_1}}\cdots(f(x+c_k))^{\frac{s_k(p-1)}{d_k}}\right).
\end{aligned}$$

Due to $d_1d_2\cdots d_k>1$, and

$$\frac{s_i(p-1)}{d_i}<p-1 \text{ for } d_i>1(i=1,2,\ldots,k),$$

from Lemma 4 we can get that the polynomial

$$(f(x+c_1))^{\frac{s_1(p-1)}{d_1}}\cdots(f(x+c_k))^{\frac{s_k(p-1)}{d_k}}$$

has a root in $\bar{\mathbb{F}}_p$ with multiples less than $p-1$, thus it can not be multiple of a $(p-1)$-th power of polynomial over $\mathbb{F}_p$. Take $g(x)=(f(x+c_1))^{\frac{s_1(p-1)}{d_1}}\cdots(f(x+c_k))^{\frac{s_k(p-1)}{d_k}}$, in Lemma 2 we have

$$\left|\sum_{\substack{x=1\\x\notin\mathcal{A}}}^{p}\chi\left(f(x+c_1)^{\frac{s_1(p-1)}{d_1}}\cdots f(x+c_k)^{\frac{s_k(p-1)}{d_k}}\right)\right| < (kl-1)p^{\frac{1}{2}}.$$

Hence, we have

$$|B_1-(p-kl)| < (2^{k\omega(p-1)}-1)(kl-1)p^{\frac{1}{2}} \le 2^{k\omega(p-1)}(kl-1)p^{\frac{1}{2}}. \tag{3.9}$$

Using the methods in the proof of Theorem 1 we have

$$g_i=\frac{1}{p^2}\sum_{m_i,n_i=1}^{p-1} e\left(\frac{m_i(f(x+c_i))+n_i\overline{f(x+c_i)}}{p}\right)U_{m_i}(u_i)U_{n_i}(v_i).$$

From the above discussion and Lemma 5, we can obtain

$$\begin{aligned}
|B_2| &< \left|\prod_{i=1}^{k}\left(\sum_{d_i|p-1}\frac{\mu(d_i)}{\phi(d_i)}\sum_{\chi_{d_i}}\sum_{\substack{x=1\\x\notin\mathcal{A}}}^{p}\chi_{d_i}(f(x+c_i))\right)\sum_{t=1}^{k}(-1)^t\sum_{i_1=1}^{k}\sum_{\substack{i_2=1\\i_1<i_2<\cdots<i_t}}^{k}\cdots\sum_{i_t=1}^{k}g_{i_1}g_{i_2}\cdots g_{i_t}\right| \\
&< \prod_{i=1}^{k}\left(\sum_{d_i|p-1}\frac{|\mu(d_i)|}{\phi(d_i)}\sum_{\chi_{d_i}}\right)\sum_{t=1}^{k}\binom{k}{t}T_p^{2t}\ln^{2t}p\cdot\left|\sum_{\substack{x=1\\x\notin\mathcal{A}}}^{p}\chi_{d_i}(f(x+c_i))\right. \\
&\quad \left.\cdot e\left(\frac{m_1(f(x+c_1))+n_1\overline{(f(x+c_1))}+\cdots+m_t(f(x+c_t))+n_t\overline{(f(x+c_t))}}{p}\right)\right| \\
&< 2^{k\omega(p-1)}\cdot\sum_{t=1}^{k}\binom{k}{t}T_p^{2t}\ln^{2t}p(kl+l)p^{\frac{1}{2}}. \qquad (3.10)
\end{aligned}$$

Combing Eqs (3.8), (3.9) and (3.10) we have

$$\begin{aligned}
&\left|M(f(x),\mathcal{R},p)-\frac{1}{2^k}\frac{\phi^k(p-1)}{(p-1)^k}(p-kl)\right| \\
<\ &\frac{1}{2^k}\frac{\phi^k(p-1)}{(p-1)^k}\left[2^{k\omega(p-1)}(kl-1)p^{\frac{1}{2}}+2^{k\omega(p-1)}\cdot\sum_{t=1}^{k}\binom{k}{t}T_p^{2t}\ln^{2t}p(kl+l)p^{\frac{1}{2}}\right] \\
=\ &\frac{1}{2^k}\frac{\phi^k(p-1)}{(p-1)^k}2^{k\omega(p-1)}p^{\frac{1}{2}}\cdot\left[(kl-1)+((k+1)l)\sum_{t=1}^{k}\binom{k}{t}T_p^{2t}\ln^{2t}p\right]. \qquad (3.11)
\end{aligned}$$

Then we have

$$M(f(x),\mathcal{R},p)=\frac{1}{2^k}\frac{\phi^k(p-1)}{(p-1)^{k-1}}+\mathrm{O}\left(\frac{\phi^k(p-1)}{p^{k-\frac{1}{2}}}2^{k\omega(p-1)}\ln^{2k}p\right).$$

This complete the proof of Theorem 2.

## 4. Conclusions

From two perspectives, this paper consider the distribution of *LPRs* that are related to the generalized Golomb's conjecture. Theorem 1 extends the binary linear equation $ag_1 + bg_2 = c$ to the multivariate linear equation $a_1g_1 + a_2g_2 + \cdots + a_kg_k = c$, and uses the properties of Gauss sums to derive an asymptotic formula for the number of its solutions $g_1, g_2, \ldots, g_k$ that are *LPRs*. Theorem 2 considers $k$ consecutive *LPRs* and employs the upper bound estimation of the generalized Kloosterman sums to provide a more general result that for $f(x) \in \mathbb{F}_p[x]$, $k$ polynomials $f(x + c_1), f(x + c_2), \ldots, f(x + c_k)$ are Lehmer primitive roots modulo $p$.

## Use of AI tools declaration

The authors declare they have not used Artificial Intelligence (AI) tools in the creation of this article.

## Acknowledgments

The author gratefully appreciates the referees and academic editor for their helpful and detailed comments.

This work is supported by the N. S. F. (12126357) of P. R. China and the Natural Science Basic Research Plan in Shaanxi Province of China (2023-JC-QN-0050).

## Conflict of interest

The author declare there are no conflicts of interest.

## References

1. E. Vegh, A note on the distribution of the primitive roots of a prime, *J. Number Theory*, **3** (1971), 13–18. https://doi.org/10.1016/0022-314X(71)90046-1
2. R. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Problem Books in Mathematics, Springer-Verlag, New York, 2004. https://doi.org/10.1007/978-0-387-26677-0_2
3. S. Cohen, Consecutive primitive roots in a finite field, *Proc. Amer. Math. Soc.*, **93** (1985), 189–197. https://doi.org/10.1090/S0002-9939-1985-0770516-9
4. S. Golomb, Algebraic constructions for Costas arrays, *J. Combin. Theory Ser. A*, **37** (1984), 13–21. https://doi.org/10.1016/0097-3165(84)90015-3
5. Q. Sun, On primitive roots in a finite field (Chinese, with English summary), *Sichuan Daxue Xuebao*, **25** (1988), 133–139.
6. S. Cohen, T. Oliveira e Silva, N. Sutherland, T. Trudgian, Linear combinations of primitive elements of a finite field, *Finite Fields Appl.*, **51** (2018), 388–406. https://doi.org/10.1016/j.ffa.2018.02.009
7. L. Carlitz, Sets of primitive roots, *Compos. Math.*, **13** (1958), 65–70.

8. E. Vegh, Pairs of consecutive primitive roots modulo a prime, *Proc. Amer. Math. Soc.*, **19** (1968), 1169–1170. https://doi.org/10.1090/S0002-9939-1968-0230680-7

9. W. Zhang, T. Wang, The primitive roots and a problem related to the Golomb conjecture, *AIMS Math.*, **5** (2020), 3899–3905. https://doi.org/10.3934/math.2020252

10. L. Carlitz, Distribution of primitive roots in a finite field, *Quart. J. Math.*, **4** (1953), 4–10. https://doi.org/10.1093/qmath/4.1.4

11. C. Cobeli, A. Zaharescu, On the distribution of primitive roots mod $p$, *Acta Arith.*, **83** (1998), 143–153. https://doi.org/10.4064/aa-83-2-143-153

12. W. Zhang, A problem of D.H.Lehmer and its generalization, *Compos. Math.*, **91** (1994), 47–51. https://doi.org/10.1007/s10114-004-0329-z

13. T. Wang, X. Wang, On Golomb's conjecture and Lehmer's numbers, *Open Math.*, **15** (2017), 1003–1009. https://doi.org/10.1515/math-2017-0083

14. S. Cohen, T. Trudgian, Lehmer numbers and primitive roots modulo a prime, *J. Number Theory*, **203** (2019), 68–79. https://doi.org/10.1016/j.jnt.2019.03.004

15. T. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976. https://doi.org/10.1007/978-1-4757-5579-4

16. W. Narkiewicz, *Classical Problems in Number Theory*, Polish Scientifc Publishers, 1986.

17. W. Schmidt, *Equations over finite fields, An elementary approach. Lecture Notes in Math. 536*, Springer, New York, 1976. https://doi.org/10.1007/BFb0080437

18. L. Goubin, C. Mauduit, A. Sárközy, Construction of large families of pseudorandom binary sequences, *J. Number Theory*, **106** (2004), 56–69. https://doi.org/10.1016/j.jnt.2003.12.002