JP Journal of Algebra, Number Theory and Applications
Volume 14, Number 1, 2009, Pages 37-50
Published Online: August 12, 2009
This paper is available online at http://www.pphmj.com

ON A GENERALIZATION OF D. H. LEHMER PROBLEM

YI YUAN and HOU YIWEI

Research Center for Science
Xi'an Jiaotong University
Xi'an, Shaanxi, P. R. China

Abstract

Let q be an odd number. For each integer x with $1 \le x \le q$ and $(x, q) = 1$, it is clear that there exists one and only one $\overline{x}$ with $0 < \overline{x} \le q$ such that $x\overline{x} \equiv 1(q)$. Let k be any fixed integer with $k \ge 2$, $\varepsilon_i = \pm 1$, $i = 1, 2, ..., k$, $N(q, k; \varepsilon_1, ..., \varepsilon_k)$ denote the number of all k-tuples with positive integer coordinates $(x_1, x_2, ..., x_k)$ such that $1 \le x_i \le q$, $(x_i, q) = 1$, $(-1)^{x_i + \overline{x_i}} = \varepsilon_i$ and $x_1 x_2 \cdots x_k \equiv 1(q)$. If $q = p$ is an odd prime and $k \ge 2$ is an even number, then we let $M(p, k; \varepsilon_1, ..., \varepsilon_k)$ denote the number of all k-tuples with primitive roots coordinates $(x_1, x_2, ..., x_k)$ such that $1 \le x_i \le p - 1$, $(-1)^{x_i + \overline{x_i}} = \varepsilon_i$ and $x_1 x_2 \cdots x_k \equiv 1(p)$. The main purpose of this paper is to use the estimates of general Kloosterman's sums and the properties of trigonometric sums to study the asymptotic behavior of the mean values $N(q, k; \varepsilon_1, ..., \varepsilon_k)$ and $M(p, k; \varepsilon_1, ..., \varepsilon_k)$, and to give two interesting asymptotic formulae.

1. Introduction

Let q be an odd number. For each integer x with $1 \le x \le q$ and $(x, q) = 1$, we

2000 Mathematics Subject Classification: 11L05, 11N07.

Keywords and phrases: Lehmer problem, trigonometric sums, asymptotic formula.

This work is supported by the N.S.F. of P. R. China (10601039).

Received January 9, 2009

know that there exists one and only one $\bar{x}$ with $0 < \bar{x} \le q$ such that $x\bar{x} \equiv 1(q)$. Let $N(q)$ be the number of cases in which x and $\bar{x}$ are of opposite parity. For $q = p$, an odd prime, D. H. Lehmer [5] asks us to find $N(p)$ or at least to say something nontrivial about it. The author [9] obtained an asymptotic formula for $N(q)$. That is,

$$N(q) = \frac{1}{2}\phi(q) + O(\sqrt{q}d(q)\ln^2 q),$$

where $\phi(q)$ is the Euler function and $d(q)$ is the divisor function.

In this paper, we consider a generalization of D. H. Lehmer problem. Let k be any fixed integer with $k \ge 2$, $\varepsilon_i = \pm 1$, $i = 1, 2, ..., k$, $N(q, k; \varepsilon_1, ..., \varepsilon_k)$ denote the number of all k-tuples with positive integer coordinates $(x_1, x_2, ..., x_k)$ such that $1 \le x_i \le q$, $(x_i, q) = 1$, $(-1)^{x_i + \overline{x_i}} = \varepsilon_i$ and $x_1 x_2 \cdots x_k \equiv 1(q)$. If $q = p$ is an odd prime and $k \ge 2$ is an even number, then we let $M(p, k; \varepsilon_1, ..., \varepsilon_k)$ denote the number of all k-tuples with primitive roots coordinates $(x_1, x_2, ..., x_k)$ such that $1 \le x_i \le p - 1$, $(-1)^{x_i + \overline{x_i}} = \varepsilon_i$ and $x_1 x_2 \cdots x_k \equiv 1(p)$.

By using the estimates for general Kloosterman's sums and the properties of trigonometric sums, we shall give an interesting asymptotic formula for $N(q, k; \varepsilon_1, ..., \varepsilon_k)$ and $M(p, k; \varepsilon_1, ..., \varepsilon_k)$. That is, we shall prove the following two main theorems:

Theorem 1. *Let q be an odd number and $k \ge 3$ be any fixed integer. Then we have the asymptotic formula*

$$N(q, k; \varepsilon_1, ..., \varepsilon_k) = \frac{1}{2^k}\phi^{k-1}(q) + O\left(q^{k-\frac{3}{2}}d^2(q)\ln^2 q\right),$$

where the constant O depends only on k.

Theorem 2. *Let p be an odd prime and k be any even number with $k \ge 4$. Then we have the asymptotic formulae*

(i) $M(p, 2; \varepsilon_1, \varepsilon_1) = \frac{1}{2}\phi(p-1) + O\left(p^{\frac{1}{2}+\varepsilon}\right)$,

(ii) $M(p, k; \varepsilon_1, ..., \varepsilon_k) = \frac{1}{2^k}\frac{\phi^k(p-1)}{p-1}\prod_{p_1 | p-1}\left(1+\frac{1}{(p_1-1)^{k-1}}\right)+O\left(p^{k-\frac{3}{2}+\varepsilon}\right),$

where ε *is any fixed positive number and* $\prod_{p_1 | p-1}$ *denotes the product over all different prime divisors of* $p-1$.

2. Several Elementary Lemmas

To complete the proof of the theorems, we need several elementary lemmas as follows. First we have

Lemma 1. *Let* $q \geq 3$ *be an integer, p be an odd prime, and m and n be integers. Then for each Dirichlet character* χ *modulo p, we have the estimates*

(i) $\sum_{a=1}^{p-1}\chi(a)e\left(\frac{ma+n\bar{a}}{p}\right) \ll (m, n, p)^{\frac{1}{2}}p^{\frac{1}{2}+\varepsilon},$

(ii) $\sum_{a=1}^{q}{}'e\left(\frac{ma+n\bar{a}}{q}\right) \ll (m, n, q)^{\frac{1}{2}}q^{\frac{1}{2}}d(q),$

where $\bar{a}$ *denotes the inverse of a modulo q, that is,* $a\bar{a} \equiv 1 \bmod q$, $e(y) = e^{2\pi iy}$ *and* (m, n, p) *denotes the greatest common divisor of m, n and p.*

Proof. These estimates can be obtained via the methods of Weil or Stepanov (see Chowla [3], Malyshev [6] and Estermann [4]).

Lemma 2. *Let a primitive root exist modulo* $n \geq 3$. *Then for each integer m with* $(m, n) = 1$, *we have the identity*

$$\sum_{k | \phi(n)}\frac{\mu(k)}{\phi(k)}\sum_{\substack{a=1\\(a,k)=1}}^{k}e\left(\frac{a \operatorname{ind} m}{k}\right) = \begin{cases}\dfrac{\phi(n)}{\phi(\phi(n))}, & \text{if } m \text{ is a primitive root of } n,\\ 0, & \text{otherwise,}\end{cases}$$

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

Proof. (See [7, Proposition 2.2]).

Lemma 3. *Let $q \geq 3$ be an odd number and p be an odd prime. Then we have the estimates*

$$\text{(i)} \quad \sum_{a=1}^{q}{}' (-1)^{a+\bar{a}} = O\left(q^{\frac{1}{2}} d(q) \ln^2 q\right),$$

$$\text{(ii)} \quad \sum_{a=1}^{p-1}{}^{*} (-1)^{a+\bar{a}} = O\left(p^{\frac{1}{2}+\varepsilon}\right),$$

where $\sum_{a}'$ denotes the summation over all a such that $(a, q) = 1$ and $\sum_{a}^{*}$ denotes the summation over all primitive roots a modulo p.

Proof. Applying the trigonometric identity

$$\sum_{a=1}^{q} e\left(\frac{an}{q}\right) = \begin{cases} q, & \text{if } q \mid n, \\ 0, & \text{if } q \nmid n, \end{cases}$$

we can get the following translation formula:

$$\begin{aligned} \sum_{a=1}^{p-1}{}^{*} (-1)^{a+\bar{a}} &= \frac{1}{p^2} \sum_{\substack{a=1 \\ a\bar{a} \equiv 1 (\mathrm{mod}\ p)}}^{p-1}{}^{*} \sum_{b=1}^{p-1}{}^{*} \sum_{c=1}^{p-1} \sum_{d=1}^{p-1} (-1)^{c+d} \\ &\quad \times \sum_{r=1}^{p} \sum_{s=1}^{p} e\left(\frac{r(a-c)}{p}\right) e\left(\frac{s(b-d)}{p}\right) \\ &= \frac{1}{p^2} \sum_{r=1}^{p} \sum_{s=1}^{p} \left(\sum_{\substack{a=1 \\ a\bar{a} \equiv 1 (\mathrm{mod}\ p)}}^{p-1}{}^{*} \sum_{b=1}^{p-1}{}^{*} e\left(\frac{ra+sb}{p}\right) \right) \\ &\quad \times \left(\sum_{c=1}^{p-1} (-1)^c e\left(\frac{-rc}{p}\right) \right) \times \left(\sum_{d=1}^{p-1} (-1)^d e\left(\frac{-sd}{p}\right) \right). \end{aligned} \tag{1}$$

Note that if $a\bar{a} \equiv 1 (p)$ and a is a primitive root mod p, then $\bar{a}$ is also a primitive root mod p. If $h \mid p-1, 1 \leq r \leq h$ and $(h, r) = 1$, then $e\left(\frac{r \operatorname{ind} a}{h}\right) = \chi(a; r, h)$ is a

Dirichlet character modulo p. So from Lemma 1 and Lemma 2, we have

$$\sum_{\substack{a=1\\ ab\equiv 1 (\mathrm{mod}\ p)}}^{p-1}{}^{*}\sum_{b=1}^{p-1}{}^{*} e\left(\frac{ra+sb}{p}\right) = \sum_{a=1}^{p-1}{}^{*} e\left(\frac{ra+s\bar{a}}{p}\right)$$

$$= \frac{\phi(p-1)}{p-1}\sum_{h\mid p-1}\frac{\mu(h)}{\phi(h)}\sum_{r=1}^{h}{}'\sum_{a=1}^{p-1}\chi(a;\ r,\ h)e\left(\frac{ra+s\bar{a}}{p}\right)$$

$$\ll \frac{\phi(p-1)}{p-1}\sum_{h\mid p-1}\frac{|\mu(h)|}{\phi(h)}\cdot\phi(h)\cdot(r,\ s,\ p)^{\frac{1}{2}}\cdot p^{\frac{1}{2}+\varepsilon}$$

$$\ll p^{\frac{1}{2}+\varepsilon}\cdot(r,\ s,\ p)^{\frac{1}{2}}. \tag{2}$$

Note that for $p\nmid r$, we have the identity

$$\sum_{c=1}^{p-1}(-1)^{c} e\left(\frac{-rc}{p}\right) = \frac{-e\left(\frac{-r}{p}\right)}{1+e\left(\frac{-r}{p}\right)}, \tag{3}$$

and the trigonometric sum estimates

$$\sum_{a=1}^{n} e(ax) \ll \min\left(n,\ \frac{1}{\|x\|}\right),$$

where $\|x\| = \min(x-[x],\ 1+[x]-x)$ and $[x]$ denotes the greatest integer $\le x$.

Combining (1), (2) and (3), we immediately get

$$\sum_{a=1}^{p-1}{}^{*}(-1)^{a+\bar{a}} \ll p^{-\frac{3}{2}+\varepsilon}\left(\sum_{r=1}^{p-1}\left|\frac{e\left(\frac{-r}{p}\right)}{1+e\left(\frac{-r}{p}\right)}\right|\right)^{2}$$

$$\ll p^{-\frac{3}{2}+\varepsilon}\left(\sum_{a=1}^{p-1}\frac{1}{\left|\cos\frac{\pi r}{p}\right|}\right)^{2}$$

$$\ll p^{-\frac{3}{2}+\varepsilon}\left(\sum_{r=1}^{p-1}\left|\frac{p}{p-2r}\right|\right)^{2} \ll p^{\frac{1}{2}+\varepsilon}.$$

This completes the proof of Lemma 3.

Using the similar method of proving (ii) of Lemma 3 and noting that the estimate (ii) of Lemma 1, we can also obtain

$$\sum_{a=1}^{q}{}' (-1)^{a+\bar{a}} = \frac{1}{q^2}\sum_{\substack{a=1\\ ab\equiv 1(\bmod q)}}^{q-1}{}'\sum_{b=1}^{q-1}{}'\sum_{c=1}^{q-1}\sum_{d=1}^{q-1}(-1)^{c+d}$$

$$\times\sum_{r=1}^{q}\sum_{s=1}^{q} e\left(\frac{r(a-c)}{q}\right)e\left(\frac{s(b-d)}{q}\right)$$

$$= \frac{1}{q^2}\sum_{r=1}^{q-1}\sum_{s=1}^{q-1}\left(\sum_{\substack{a=1\\ ab\equiv 1(\bmod q)}}^{q-1}{}'\sum_{b=1}^{q-1}{}' e\left(\frac{ra+sb}{q}\right)\right)$$

$$\times\left(\sum_{c=1}^{q-1}(-1)^c e\left(\frac{-rc}{q}\right)\right)\times\left(\sum_{d=1}^{q-1}(-1)^d e\left(\frac{-sd}{q}\right)\right). \tag{4}$$

From Lemma 1, (3) and (4), we immediately get

$$\sum_{a=1}^{q}{}' (-1)^{a+\bar{a}} = \frac{1}{q^2}\sum_{r=1}^{q-1}\sum_{s=1}^{q-1}(r,\ s,\ q)^{\frac{1}{2}} q^{\frac{1}{2}} d(q)\frac{1}{\left|\cos\frac{\pi r}{q}\right|}\frac{1}{\left|\cos\frac{\pi s}{q}\right|}$$

$$\ll \frac{1}{q^2}\sum_{u\mid q}\sum_{r=1}^{\frac{q-1}{u}}\sum_{s=1}^{\frac{q-1}{u}} u^{\frac{1}{2}} q^{\frac{1}{2}} d(q)\frac{1}{\left|\cos\frac{\pi r}{q/u}\right|}\frac{1}{\left|\cos\frac{\pi s}{q/u}\right|}$$

$$\ll \frac{1}{q^2}\sum_{u\mid q}\sum_{r=1}^{\frac{q-1}{u}}\sum_{s=1}^{\frac{q-1}{u}} u^{\frac{1}{2}} q^{\frac{1}{2}} d(q)\frac{q/u}{\left|\frac{q}{u}-2r\right|}\frac{q/u}{\left|\frac{q}{u}-2s\right|}$$

$$\ll \sum_{u\mid q}\frac{d(q)q^{\frac{1}{2}}}{u^{\frac{3}{2}}}\ln^2 q \ll q^{\frac{1}{2}} d(q)\ln^2 q.$$

This proves the (ii) of Lemma 3.

Lemma 4. *Let p be an odd prime and k be a positive even number. Then we have the identity*

$$\sum_{\substack{x_1=1 \\ x_1\cdots x_k\equiv 1 (\mathrm{mod}\ p)}}^{p-1*} \cdots \sum_{x_k=1}^{p-1*} 1 = \frac{\phi^k(p-1)}{p-1} \prod_{p_1 \mid p-1} \left(1 + \frac{1}{(p_1-1)^{k-1}}\right).$$

Proof. From the orthogonality properties of character sums modulo p and Lemma 2, we have

$$\sum_{\substack{x_1=1 \\ x_1x_2\cdots x_k\equiv 1 (\mathrm{mod}\ p)}}^{p-1*} \sum_{x_2=1}^{p-1*} \cdots \sum_{x_k=1}^{p-1*} 1 = \frac{1}{p-1} \sum_{\chi \bmod p} \left(\sum_{a=1}^{p-1*} \chi(a)\right)^k$$

$$= \frac{1}{p-1} \sum_{\chi \bmod p} \left(\frac{\phi(p-1)}{p-1} \sum_{h \mid p-1} \frac{\mu(h)}{\phi(h)} \sum_{r=1}^{h}{}' \sum_{a=1}^{p-1} \chi(a)\chi(a; r, h) \right)^k. \quad (5)$$

In expression (5), for any fixed χ modulo p, there exists one and only one pair of h, r with $1 \le r \le h$ and $(r, h) = 1$ such that $\chi(a; r, h) = \overline{\chi}(a)$. For each h, there are exact $\phi(h)$ numbers r such that $1 \le r \le h$ and $(h, r) = 1$. Thus we have

$$\sum_{\substack{x_1=1 \\ x_1x_2\cdots x_k\equiv 1 (\mathrm{mod}\ p)}}^{p-1*} \sum_{x_2=1}^{p-1*} \cdots \sum_{x_k=1}^{p-1*} 1 = \frac{1}{p-1} \sum_{h \mid p-1} \sum_{r=1}^{h}{}' \left(\phi(p-1) \cdot \frac{\mu(h)}{\phi(h)}\right)^k$$

$$= \frac{1}{p-1} \sum_{h \mid p-1} \phi(h) \cdot \left(\phi(p-1) \cdot \frac{\mu(h)}{\phi(h)}\right)^k$$

$$= \frac{\phi^k(p-1)}{p-1} \prod_{p_1 \mid p-1} \left(1 + \frac{(-1)^k}{\phi^{k-1}(p_1)}\right)$$

$$= \frac{\phi^k(p-1)}{p-1} \prod_{p_1 \mid p-1} \left(1 + \frac{1}{(p_1-1)^{k-1}}\right).$$

This proves Lemma 4.

Lemma 5. *Let $q \geq 3$ be an odd number and p be an odd prime. Then for any positive integer $k \geq 3$, we have the estimates*

(i) $$\sideset{}{'}\sum_{\substack{x_1=1\\ x_1\cdots x_k\equiv 1(\mathrm{mod}\, q)}}^{q} \cdots \sideset{}{'}\sum_{x_k=1}^{q} \prod_{i=1}^{k} \varepsilon_i (-1)^{x_i+\overline{x_i}} \ll q^{k-\frac{3}{2}} d^2(q) \ln q,$$

(ii) $$\sideset{}{^*}\sum_{\substack{x_1=1\\ x_1\cdots x_k\equiv 1(\mathrm{mod}\ p)}}^{p-1} \cdots \sideset{}{^*}\sum_{x_k=1}^{p-1} \prod_{i=1}^{k} \varepsilon_i (-1)^{x_i+\overline{x_i}} \ll p^{\frac{k}{2}+\varepsilon}.$$

Proof. From the congruence properties and the trigonometric inequality, we can get

$$\begin{aligned}
\sideset{}{'}\sum_{\substack{x_1=1\\ x_1\cdots x_k\equiv 1(\mathrm{mod}\, q)}}^{q} \cdots \sideset{}{'}\sum_{x_k=1}^{q} \prod_{i=1}^{k} \varepsilon_i (-1)^{x_i+\overline{x_i}} &\ll \sideset{}{'}\sum_{u=1}^{q} \left| \sum_{x_1\cdots x_{k-2}\equiv u(\mathrm{mod}\, q)} (-1)^{x_1+\cdots+x_{k-2}+\overline{x_1}+\cdots+\overline{x}_{k-2}} \right| \\
&\quad \times \left| \sum_{x_{k-1}x_k\equiv \overline{u}(\mathrm{mod}\, q)} (-1)^{x_{k-1}+x_k+\overline{x}_{k-1}+\overline{x}_k} \right| \\
&\ll \phi^{k-3}(q) \sideset{}{'}\sum_{u=1}^{q} \left| \sum_{x_1x_2\equiv u(\mathrm{mod}\, q)} (-1)^{x_1+x_2+\overline{x}_1+\overline{x}_2} \right| \\
&\ll \phi^{k-3}(q) \sideset{}{'}\sum_{u=1}^{q} \left| \sideset{}{'}\sum_{x_1=1}^{q} (-1)^{x_1(1+\overline{u})+\overline{x}_1(1+u)} \right| \\
&\ll \phi^{k-3}(q) \sideset{}{'}\sum_{u=1}^{q} \left| \sideset{}{'}\sum_{a=1}^{q} e\Big(\frac{a(1+\overline{u})+\overline{a}(1+u)}{q}\Big) \right| \\
&\ll \phi^{k-3}(q) \sideset{}{'}\sum_{u=1}^{q} (1+\overline{u}, 1+u, q)^{\frac{1}{2}} \cdot q^{\frac{1}{2}} \cdot d(q). \qquad (6)
\end{aligned}$$

Note that $(u, q) = (\bar{u}, q) = 1$, thus $(1+u, q) = (u\bar{u}+u, q) = (1+\bar{u}, q)$. So from this and (6), we get

$$\sum_{\substack{x_1=1\\ x_1\cdots x_k\equiv 1(\mathrm{mod}\, q)}}^{q}{}' \cdots \sum_{x_k=1}^{q}{}' \prod_{i=1}^{k} \varepsilon_i (-1)^{x_i+\overline{x_i}} \ll \phi^{k-3}(q) \sum_{u=1}^{q}{}' (1+u, q)^{\frac{1}{2}} \cdot q^{\frac{1}{2}} \cdot d(q)$$

$$\ll \phi^{k-3}(q) \cdot q^{\frac{1}{2}} d(q) \sum_{d\mid q} d^{\frac{1}{2}} \sum_{\substack{u=1\\ d\mid u+1}}^{q}{}' 1$$

$$\ll \phi^{k-3}(q) \cdot q^{\frac{1}{2}} d(q) \sum_{d\mid q} d^{\frac{1}{2}} \cdot \frac{q}{d}$$

$$\ll q^{k-\frac{3}{2}} d^2(q) \ln q.$$

This proves the (i) of Lemma 5.

Using the orthogonality relation for character sums mod p, we have the following translation formula:

$$\sum_{\substack{x_1=1\\ x_1\cdots x_k\equiv 1(\mathrm{mod}\, p)}}^{p-1}{}^{*} \cdots \sum_{x_k=1}^{p-1}{}^{*} \prod_{i=1}^{k} \varepsilon_i (-1)^{x_i+\overline{x_i}} = \frac{1}{p-1} \sum_{\chi \bmod p} \left(\sum_{a=1}^{p-1}{}^{*} \chi(a)(-1)^{a+\bar{a}} \right)^k. \tag{7}$$

Using the similar method of proving Lemma 3, we can also prove that

$$\sum_{a=1}^{p-1}{}^{*} \chi(a)(-1)^{a+\bar{a}} \ll p^{\frac{1}{2}+\varepsilon}. \tag{8}$$

From (7) and (8), we obtain

$$\sum_{\substack{x_1=1\\ x_1\cdots x_k\equiv 1(\mathrm{mod}\, p)}}^{p-1}{}^{*} \cdots \sum_{x_k=1}^{p-1}{}^{*} \prod_{i=1}^{k} \varepsilon_i (-1)^{x_i+\overline{x_i}} \ll p^{\frac{k}{2}+\varepsilon}.$$

This completes the proof of Lemma 5.

Lemma 6. *Let $k \geq 3$ be an integer. Then for any fixed integer m with $1 \leq m \leq k-1$, we have the estimates*

$$\sideset{}{^*}\sum_{\substack{x_1=1\\ x_1\cdots x_k\equiv 1(\mathrm{mod}\ p)}}^{p-1}\cdots\sideset{}{^*}\sum_{x_k=1}^{p-1}\prod_{i=1}^{k-m}\varepsilon_i(-1)^{x_i+\overline{x_i}} \ll p^{\frac{k+m}{2}-1+\varepsilon},$$

where ε is any fixed positive number.

Proof. From (8) and Lemma 2, we have

$$\sideset{}{^*}\sum_{\substack{x_1=1\\ x_1\cdots x_k\equiv 1(\mathrm{mod}\ p)}}^{p-1}\cdots\sideset{}{^*}\sum_{x_k=1}^{p-1}\prod_{i=1}^{k-m}\varepsilon_i(-1)^{x_i+\overline{x_i}}$$

$$= \frac{1}{p-1}\sum_{\chi \bmod p}\left(\sideset{}{^*}\sum_{a=1}^{p-1}\chi(a)\right)^m\cdot\left(\sideset{}{^*}\sum_{b=1}^{p-1}\chi(b)(-1)^{b+\bar{b}}\right)^{k-m}$$

$$\ll \frac{1}{p-1}\sum_{\chi \bmod p}\left|\frac{\phi(p-1)}{p-1}\sum_{h\mid p-1}\frac{\mu(h)}{\phi(h)}\sideset{}{'}\sum_{u=1}^{h}\sum_{a=1}^{p-1}\chi(a)\chi(a;\,u,\,h)\right|^m\cdot p^{\frac{k-m}{2}+\varepsilon}$$

$$\ll \frac{1}{p-1}\sum_{h\mid p-1}\phi(h)\cdot\left|\phi(p-1)\cdot\frac{\mu(h)}{\phi(h)}\right|^m\cdot p^{\frac{k-m}{2}+\varepsilon}$$

$$\ll p^{\frac{k-m}{2}-1+\varepsilon}\cdot\phi^m(p-1)\cdot\sum_{h\mid p-1}\frac{1}{\phi^{m-1}(h)}$$

$$\ll p^{\frac{k+m}{2}-1+\varepsilon}.$$

This proves Lemma 6.

3. Proof of the Theorems

From the several lemmas on the above section, we can easily give the proof of the theorems. In fact for $k \geq 3$, applying Lemma 2, Lemma 3 and Lemma 5, we get

$$N(q, k; \varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k)$$

$$= \frac{1}{2^k} \sum_{\substack{x_1=1 \\ x_1 \cdots x_k \equiv 1 (\mathrm{mod}\, q)}}^{q}{}' \cdots \sum_{x_k=1}^{q}{}' \prod_{i=1}^{k} (1 + \varepsilon_i (-1)^{x_i + \overline{x_i}})$$

$$= \frac{1}{2^k} \sum_{\substack{x_1=1 \\ x_1 \cdots x_k \equiv 1 (\mathrm{mod}\, q)}}^{q}{}' \cdots \sum_{x_k=1}^{q}{}' \left(1 + \sum_{i=1}^{k} \varepsilon_i (-1)^{x_i + \overline{x_i}} + \cdots + \sum_{i=1}^{k} \varepsilon_i (-1)^{x_i + \overline{x_i}}\right)$$

$$= \frac{1}{2^k} \sum_{\substack{x_1=1 \\ x_1 \cdots x_k \equiv 1 (\mathrm{mod}\, q)}}^{q}{}' \cdots \sum_{x_k=1}^{q}{}' 1 + \frac{1}{2^k} \sum_{\substack{x_1=1 \\ x_1 \cdots x_k \equiv 1 (\mathrm{mod}\, q)}}^{q}{}' \cdots \sum_{x_k=1}^{q}{}' \sum_{i=1}^{k} \varepsilon_1 (-1)^{x_i + \overline{x_i}}$$

$$+ \cdots + \frac{1}{2^k} \sum_{\substack{x_1=1 \\ x_1 \cdots x_k \equiv 1 (\mathrm{mod}\, q)}}^{q}{}' \cdots \sum_{x_k=1}^{q}{}' \prod_{i=1}^{k} \varepsilon_i (-1)^{x_i + \overline{x_i}}$$

$$= \frac{\phi^{k-1}(q)}{2^k} + \frac{\phi^{k-2}(q)}{2^k} \sum_{i=1}^{k} \sum_{x_i=1}^{q}{}' \varepsilon_i (-1)^{x_i + \overline{x_i}}$$

$$+ \cdots + \frac{1}{2^k} \sum_{\substack{x_1=1 \\ x_1 \cdots x_k \equiv 1 (\mathrm{mod}\, q)}}^{q}{}' \cdots \sum_{x_k=1}^{q}{}' \prod_{i=1}^{k} \varepsilon_i (-1)^{x_i + \overline{x_i}}$$

$$= \frac{\phi^{k-1}(q)}{2^k} + O\left(q^{k-2} \cdot q^{\frac{1}{2}} d^2(q) \ln^2 p\right)$$

$$+ \cdots + O\left(q^{k-\frac{3}{2}} d^2(q) \ln p\right)$$

$$= \frac{\phi^{k-1}(q)}{2^k} + O\left(q^{k-\frac{3}{2}} d^2(q) \ln^2 q\right). \tag{9}$$

If $k = 2,$ then by using the (i) of Lemma 3, we can easily get

$$N(q, 2; \varepsilon_1, \varepsilon_1) = \frac{1}{2^2} \sum_{\substack{x_1=1 \\ x_1 x_2 \equiv 1 (\mathrm{mod}\, q)}}^{q}{}' \sum_{x_2=1}^{q}{}' (1 + \varepsilon_1(-1)^{x_1+\overline{x_1}})(1 + \varepsilon_1(-1)^{x_2+\overline{x_2}})$$

$$= \frac{1}{2^2} \sum_{x_1=1}^{q}{}' (1 + \varepsilon_1(-1)^{x_1+\overline{x_1}})^2$$

$$= \frac{1}{2} \sum_{x_1=1}^{q}{}' (1 + \varepsilon_1(-1)^{x_1+\overline{x_1}})$$

$$= \frac{1}{2}\phi(q) + O\left(\sum_{x_1=1}^{q}{}' (-1)^{x_1+\overline{x_1}} \right)$$

$$= \frac{1}{2}\phi(q) + O\left(q^{\frac{1}{2}} d(q) \ln^2 q \right).$$

This completes the proof of Theorem 1.

For even number $k \geq 4$ and any primitive root $x_i \bmod p$, note that the identity

$$\frac{1}{2}(1 + \varepsilon_i(-1)^{x_i+\overline{x_i}}) = \begin{cases} 1, & \text{if } (-1)^{x_i+\overline{x_i}} = \varepsilon_i, \\ 0, & \text{otherwise,} \end{cases}$$

we have

$$M(p, k; \varepsilon_1, \varepsilon_2, ..., \varepsilon_k) = \frac{1}{2^k} \sum_{\substack{x_1=1 \\ x_1 \cdots x_k \equiv 1 (\mathrm{mod}\, p)}}^{p-1}{}^{*} \cdots \sum_{x_k=1}^{p-1}{}^{*} \prod_{i=1}^{k} (1 + \varepsilon_i(-1)^{x_i+\overline{x_i}})$$

$$= \frac{1}{2^k} \sum_{\substack{x_1=1 \\ x_1 \cdots x_k \equiv 1 (\mathrm{mod}\, p)}}^{p-1}{}^{*} \cdots \sum_{x_k=1}^{p-1}{}^{*} \left(1 + \sum_{i=1}^{k} \varepsilon_i(-1)^{x_i+\overline{x_i}} + \cdots + \prod_{i=1}^{k} \varepsilon_i(-1)^{x_i+\overline{x_i}} \right)$$

$$= \frac{1}{2^k} \sideset{}{^*}\sum_{\substack{x_1=1 \\ x_1 \cdots x_k \equiv 1 (\mathrm{mod}\ p)}}^{p-1} \cdots \sideset{}{^*}\sum_{x_k=1}^{p-1} 1 + \frac{1}{2^k} \sideset{}{^*}\sum_{\substack{x_1=1 \\ x_1 \cdots x_k \equiv 1 (\mathrm{mod}\ p)}}^{p-1} \cdots \sideset{}{^*}\sum_{x_k=1}^{p-1} \sum_{i=1}^{k} \varepsilon_1 (-1)^{x_i + \overline{x_i}}$$

$$+ \cdots + \frac{1}{2^k} \sideset{}{^*}\sum_{\substack{x_1=1 \\ x_1 \cdots x_k \equiv 1 (\mathrm{mod}\ p)}}^{p-1} \cdots \sideset{}{^*}\sum_{x_k=1}^{p-1} \prod_{i=1}^{k} \varepsilon_i (-1)^{x_i + \overline{x_i}}$$

$$= \frac{\phi^k(p)}{p-1} \prod_{p_1 \mid p-1} \left(1 + \frac{1}{\phi^{k-1}(p_1)}\right) + O\left(p^{k-\frac{3}{2}+\varepsilon}\right).$$

This proves the (ii) of Theorem 2.

If $k = 2$ and $\varepsilon_1 = \varepsilon_2$, then from (ii) of Lemma 3, we have

$$M(p, k; \varepsilon_1, \varepsilon_1) = \frac{1}{2^2} \sideset{}{^*}\sum_{\substack{a=1 \\ ab \equiv 1 (\mathrm{mod}\ p)}}^{p-1} \sideset{}{^*}\sum_{b=1}^{p-1} (1 + \varepsilon_1 (-1)^{a+\overline{a}})(1 + \varepsilon_1 (-1)^{b+\overline{b}})$$

$$= \frac{1}{2^2} \sideset{}{^*}\sum_{a=1}^{p-1} (1 + \varepsilon_1 (-1)^{a+\overline{a}})^2$$

$$= \frac{1}{2} \sideset{}{^*}\sum_{a=1}^{p-1} (1 + \varepsilon_1 (-1)^{a+\overline{a}})$$

$$= \frac{1}{2} \phi(p-1) + O\left(p^{\frac{1}{2}+\varepsilon}\right).$$

This completes the proof of Theorem 2.

References

[1] Tom M. Apostol, Introduction to Analytic Number Theory, Springer-Verlag, New York, 1976.

[2] E. Bombieri, On exponential sums in finite fields, Amer. J. Math. 88 (1966), 71-105.

[3] S. Chowla, On Kloosterman's sum, Norske Vid. Selsk. Forh. (Trondheim) 40 (1967), 70-72.

[4] T. Estermann, On Kloosterman's sum, Mathematika 8 (1961), 83-86.

[5] Richard K. Guy, Unsolved Problems in Number Theory, Springer-Verlag, New York, 1981, pp. 139-140.

[6] A. V. Malyshev, A generalization of Kloosterman sums and their estimates, Vestnik Leningrad Univ. 15 (1960), 59-75 (in Russian).

[7] Wladyslaw Narkiewicz, Classical Problems in Number Theory, PWN-Polish Scientific Publishers, Warszawa, 1987, pp. 79-80.

[8] Wolfgang M. Schmidt, Equation over finite fields, Lectures Notes in Mathematics 536, Springer-Verlag, Berlin, 1976.

[9] Zhang Wenpeng, A problem of D. H. Lehmer and its generalization. II, Compos. Math. 91 (1994), 47-56.