Publ. Math. Debrecen
53 / 3-4 (1998), 245–255

On the distribution of primitive roots modulo p

By WENPENG ZHANG (Xi'an)

Abstract. Let $p \geq 3$ be a prime. For each primitive root x modulo p with $1 \leq x \leq p-1$, it is clear that there exists one and only one primitive root $\overline{x}$ modulo p with $1 \leq \overline{x} \leq p-1$ such that $x\overline{x} \equiv 1 \mod p$. Let σ be a fixed positive number with $0 \leq \sigma \leq 1$, $\mathcal{A}$ denotes the set of all primitive roots modulo p in interval $[1, p]$. The main purpose of this paper is to study the asymptotic properties of the mean value

$$M(p, k, \sigma) = \sum_{\substack{a \in \mathcal{A} \\ ab \equiv 1 (p) \\ |a-b| < \sigma p}} \sum_{b \in \mathcal{A}} |a-b|^k$$

and give an interesting asymptotic formula.

1. Introduction

Let $p \geq 3$ be a prime. It is clear that for each primitive root x modulo p with $1 \leq x \leq p-1$, the integer $\overline{x}$ defining by $x\overline{x} \equiv 1 \pmod{p}$ and $1 \leq \overline{x} \leq p-1$ is also a primitive root modulo p. Let $0 \leq \sigma \leq 1$ be a fixed real number, $\mathcal{A} = \mathcal{A}(p)$ denotes the set of all primitive roots modulo p in the interval $[1, p]$, and define $M(p, k, \sigma)$ as follows

$$M(p, k, \sigma) = \sum_{\substack{a \in \mathcal{A} \\ ab \equiv 1 (p) \\ |a-b| < \sigma p}} \sum_{b \in \mathcal{A}} |a-b|^k \tag{1}$$

where k be any fixed non-negative real number. The main purpose of this paper is to study the asymptotic properties of (1). About this problem, it

Mathematics Subject Classification: 11N69, 11L05.
Key words and phrases: primitive roots, mean value, asymptotic formula.

seems that no one has studied it yet, at least I have not seen expressions like (1) before. The problem is interesting because it can help us to find how large the difference is between a primitive root and its inverse modulo p. In this paper, we use the estimates for general Kloosterman sum and trigonometric sum to study the asymptotic behaviour of (1), and give a sharper asymptotic formula for $M(P, K, \sigma)$ for any fixed real number $0 \leq \sigma \leq 1$ and $k \geq 0$. That is, we shall prove the following two main conclusions:

Theorem 1. *Let $p \geq 3$ be a prime. Then for any fixed $0 \leq \sigma \leq 1$ and $k \geq 0$, we have the asymptotic formula*

$$M(p, k, \sigma) = 2\phi(p-1)p^k \left(\frac{\sigma^{k+1}}{k+1} - \frac{\sigma^{k+2}}{k+2} \right) + O\left(p^{k+\frac{1}{2}+\epsilon}\right)$$

where $\phi(n)$ is the Euler function and ϵ is any fixed positive number.

Theorem 2. *Let $p \geq 3$ be a prime. Then for any integer m with $1 \leq m \leq \sqrt{p}$ and fixed positive number ϵ, we have*

$$\begin{aligned} &\#\{a : a \in \mathcal{A},\ \overline{a} \in \mathcal{A},\ a\overline{a} \equiv 1 \pmod{p},\ a \equiv \overline{a} \pmod{m}\} \\ &= \frac{\phi(p-1)}{m} + O\left(p^{\frac{1}{2}+\epsilon}\right) \end{aligned}$$

where $\#\{\ldots\ldots\}$ denotes the number of the elements in set $\{\ldots\ldots\}$.

From the Theorem 1, we may immediately deduce the following two corollaries:

Corollary 1. *Let $p \geq 3$ be a prime. Then for any fixed positive number $0 \leq \sigma \leq 1$ and $\epsilon > 0$ we have*

$$\sum_{\substack{a \in \mathcal{A} \\ ab \equiv 1 (p) \\ |a-b| < \sigma p}} \sum_{b \in \mathcal{A}} 1 = \phi(p-1)\sigma(2-\sigma) + O(p^{\frac{1}{2}+\epsilon}).$$

Corollary 2. *For any odd prime p and fixed positive number k, we have the asymptotic formula*

$$\sum_{\substack{a \in \mathcal{A} \\ ab \equiv 1 (p)}} \sum_{b \in \mathcal{A}} |a-b|^k = \frac{2\phi(p-1)}{(k+1)(k+2)} p^k + O(p^{k+\frac{1}{2}+\epsilon}).$$

2. Several elementary lemmas

To complete the proof of the theorems, we need some elementary lemmas. First we have

Lemma 1. *Let $p \geq 3$ be a prime, m and n be integers. Then for each Dirichlet character χ modulo p, we have the estimate*

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

where $\overline{a}$ denotes the inverse of a modulo p. That is, $a\overline{a} \equiv 1 \mod p$. ϵ is any fixed positive number, $e(y) = e^{2\pi i y}$ and (m, n, p) denotes the greatest common factor of m, n and p.

Proof. This estimate can be obtained via the methods of Weil or Stepanov (see S. Chowla [2] or A. V. Malyshev [7]).

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

$$\sum_{k|\phi(n)} \frac{\mu(k)}{\phi(k)} \sum_{\substack{a=1 \\ (a,k)=1}}^{k} e\left(\frac{a \operatorname{ind} m}{k}\right)$$

$$= \begin{cases} \frac{\phi(n)}{\phi(\phi(n))}, & \text{if } m \text{ is a primitive root of } n; \\ 0, & \text{otherwise.} \end{cases}$$

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

Proof. (See Proposition 2.2 of reference [4].)

Lemma 3. *Let $p \geq 3$ be a prime, $\mathcal{A}$ denotes the set of all primitive roots modulo p in the interval $[1, p]$. Then for any integer u, v, and m with $m \nmid u$, $m \nmid v$ we have*

$$\sum_{\substack{a \in \mathcal{A} \\ ab \equiv 1 (p)}} \sum_{b \in \mathcal{A}} e\left(\frac{ua + vb}{m}\right)$$

$$= \frac{\phi(p-1)}{p^2} e\left(\frac{(u+v)(p+1)}{2m}\right) \frac{\sin\left(\frac{\pi p u}{m}\right) \sin\left(\frac{\pi p v}{m}\right)}{\sin\left(\frac{\pi u}{m}\right) \sin\left(\frac{\pi v}{m}\right)} + O(p^{\frac{1}{2}+\epsilon})$$

where ϵ is any fixed positive number.

PROOF. Applying the trigonometric identity

$$\sum_{a=1}^{q} e\left(\frac{an}{q}\right) = \begin{cases} q, & q \mid n; \\ 0, & q \nmid n. \end{cases} \tag{2}$$

we can get the following translations

$$\begin{aligned} \sum_{\substack{a\in\mathcal{A}\\ ab\equiv 1(p)}} \sum_{b\in\mathcal{A}} e\left(\frac{au+bv}{m}\right) &= \frac{1}{p^2}\sum_{r,s=1}^{p} \sum_{\substack{a\in\mathcal{A}\\ ab\equiv 1(p)}} \sum_{b\in\mathcal{A}} e\left(\frac{ra+sb}{p}\right) \\ &\quad \times \left(\sum_{c=1}^{p} e\left(\frac{uc}{m}-\frac{rc}{p}\right)\right)\left(\sum_{d=1}^{p} e\left(\frac{vd}{m}-\frac{sd}{p}\right)\right) \\ &= \frac{\phi(p-1)}{p^2}\left(\sum_{c=1}^{p} e\left(\frac{uc}{m}\right)\right)\left(\sum_{d=1}^{p} e\left(\frac{vd}{m}\right)\right) \\ &\quad + \frac{1}{p^2}\sum_{r=1}^{p-1}\left(\sum_{\substack{a\in\mathcal{A}\\ ab\equiv 1(p)}} \sum_{b\in\mathcal{A}} e\left(\frac{ra}{p}\right)\right)\left(\sum_{c=1}^{p} e\left(\frac{uc}{m}-\frac{rc}{p}\right)\right) \\ &\quad \times \left(\sum_{d=1}^{p} e\left(\frac{vd}{m}\right)\right) + \frac{1}{p^2}\sum_{s=1}^{p-1}\left(\sum_{\substack{a\in\mathcal{A}\\ ab\equiv 1(p)}} \sum_{b\in\mathcal{A}} e\left(\frac{sb}{p}\right)\right) \\ &\quad \times \left(\sum_{c=1}^{p} e\left(\frac{uc}{m}\right)\right)\left(\sum_{d=1}^{p} e\left(\frac{vd}{m}-\frac{ds}{p}\right)\right) \\ &\quad + \frac{1}{p^2}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left(\sum_{\substack{a\in\mathcal{A}\\ ab\equiv 1(p)}} \sum_{b\in\mathcal{A}} e\left(\frac{ra+sb}{p}\right)\right) \\ &\quad \times \left(\sum_{c=1}^{p} e\left(\frac{uc}{m}-\frac{vc}{p}\right)\right)\left(\sum_{d=1}^{p} e\left(\frac{vd}{m}-\frac{ds}{p}\right)\right) \\ &\equiv A+B+C+D \end{aligned} \tag{3}$$

Main term

$$A = \frac{\phi(p-1)}{p^2}\, e\left(\frac{u}{m}\right)\frac{e\left(\frac{pu}{m}\right)-1}{e\left(\frac{u}{m}\right)-1}\cdot e\left(\frac{v}{m}\right)\frac{e\left(\frac{pv}{m}\right)-1}{e\left(\frac{v}{m}\right)-1} \tag{4}$$

$$= \frac{\phi(p-1)}{p^2}\, e\left(\frac{(u+v)(p+1)}{2m}\right) \frac{\sin\left(\frac{\pi p u}{m}\right)\sin\left(\frac{\pi p v}{m}\right)}{\sin\left(\frac{\pi u}{m}\right)\sin\left(\frac{\pi v}{m}\right)}.$$

Now we shall estimate the error terms B, C, and D respectively. Without loss of generality we can assume $m > 1$, $0 < u < m$, $0 < v < m$. Using the Lemma 1, Lemma 2, and note that the estimate

$$\sum_{u=1}^{n} e\left(\frac{au}{m}\right) = O\left(\min\left(n, \frac{1}{\|\frac{u}{m}\|}\right)\right).$$

(where $\|x\| = \min(x - [x], 1 - x + [x])$, $[x]$ be the greatest integers $\le x$). We have

$$\begin{aligned}
(5)\quad B &= \frac{1}{p^2}\sum_{r=1}^{p-1}\left(\sum_{\substack{a\in\mathcal{A}\\ ab\equiv 1(p)}}\sum_{b\in\mathcal{A}} e\left(\frac{ra}{p}\right)\right)\left(\sum_{c=1}^{p} e\left(\frac{uc}{m}-\frac{rc}{p}\right)\right)\\
&\quad\times\left(\sum_{d=1}^{p} e\left(\frac{vd}{m}\right)\right)\\
&\ll \frac{1}{p^2}\sum_{r=1}^{p-1}\left|\frac{\phi(p-1)}{p-1}\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{x=1}^{k}{}'\sum_{a=1}^{p-1} e\left(\frac{x\,\mathrm{ind}\,a}{k}\right) e\left(\frac{ra}{p}\right)\right|\\
&\quad\times\min\left(p, \frac{1}{\|\frac{u}{m}-\frac{r}{p}\|}\right)\cdot p\\
&\ll \frac{1}{p}\sum_{r=1}^{p-1}\left|\frac{\phi(p-1)}{p-1}\sum_{k|p-1}\frac{\mu(k)}{\phi(k)}\sum_{x=1}^{k}{}'\sum_{a=1}^{p-1}\chi(a;x,k) e\left(\frac{ra}{p}\right)\right|\\
&\quad\times\min\left(p, \frac{1}{\|\frac{u}{m}-\frac{r}{p}\|}\right)\\
&\ll \frac{1}{p}\sum_{r=1}^{p-1}\sqrt{p}\cdot\sum_{k|p-1}|\mu(k)|\cdot\min\left(p, \frac{1}{\|\frac{u}{m}-\frac{r}{p}\|}\right)\\
&\ll \frac{2^{\omega(p-1)}}{\sqrt{p}}\left(p+\sum_{\substack{r=1\\ |\frac{pu}{m}-r|\ge 1}}^{p-1}\frac{p}{|\frac{pu}{m}-r|}+\sum_{\substack{r=1\\ |\frac{(u\pm m)p}{m}-r|\ge 1}}^{p-1}\frac{p}{\left|\frac{(u\pm m)p}{m}-r\right|}\right)
\end{aligned}$$

$$\ll \sqrt{p}\cdot 2^{\omega(p-1)}\sum_{r=1}^{p-1}\frac{1}{r}\ll p^{\frac{1}{2}+\epsilon}$$

where $\chi(a;x,k)$ be the Dirichlet character modulo p, $\sum_{a=1}^{p-1}\chi(a;x,k)e\left(\frac{ra}{p}\right)$ be the Gauss sum and $\left|\sum_{a=1}^{p-1}\chi(a;x,k)e\left(\frac{ra}{p}\right)\right|\ll\sqrt{p}$, $\omega(n)$ denotes the number of all distinct prime divisors of n, ϵ be any fixed positive number and $\sum_{x=1}^{\prime k}$ denotes the summation over all $1\le x\le k$ such that $(x,k)=1$.

Similarly

$$C=\frac{1}{p^2}\sum_{s=1}^{p-1}\left(\sum_{\substack{a\in\mathcal{A}\\ab\equiv1(p)}}\sum_{b\in\mathcal{A}}e\left(\frac{sb}{p}\right)\right)\left(\sum_{c=1}^{p}e\left(\frac{uc}{m}\right)\right)\times\left(\sum_{d=1}^{p}e\left(\frac{vd}{m}-\frac{ds}{p}\right)\right)\ll p^{\frac{1}{2}+\epsilon}\tag{6}$$

To estimate D, we first must estimate $\sum\limits_{\substack{a\in\mathcal{A}\\ab\equiv1(p)}}\sum\limits_{b\in\mathcal{A}}e\left(\frac{ra+sb}{p}\right)$, $1\le r$, $s\le p-1$. Using the Lemma 1 and Lemma 2 we can get

$$\begin{aligned}\sum_{\substack{a\in\mathcal{A}\\ab\equiv1(p)}}\sum_{b\in\mathcal{A}}e\left(\frac{ra+sb}{p}\right)&=\frac{\phi^2(p-1)}{(p-1)^2}\sum_{k|p-1}\sum_{h|p-1}\frac{\mu(k)\mu(h)}{\phi(k)\phi(h)}\\&\quad\times\sum_{x=1}^{k}{}^{\prime}\sum_{y=1}^{h}{}^{\prime}\sum_{\substack{a=1\\ab\equiv1(p)}}^{p-1}\sum_{b=1}^{p-1}e\left(\frac{x\,\mathrm{ind}\,a}{k}+\frac{y\ \mathrm{ind}\ b}{h}\right)e\left(\frac{ra+sb}{p}\right)\\&=\frac{\phi^2(p-1)}{(p-1)^2}\sum_{k|p-1}\sum_{h|p-1}\frac{\mu(k)\mu(h)}{\phi(k)\phi(h)}\\&\quad\times\sum_{x=1}^{k}{}^{\prime}\sum_{y=1}^{h}{}^{\prime}\sum_{\substack{a=1\\ab\equiv1(p)}}^{p-1}\sum_{b=1}^{p-1}\chi(a;x,k)\chi(b;y,h)e\left(\frac{ra+sb}{p}\right)\\&=\frac{\phi^2(p-1)}{(p-1)^2}\sum_{k|p-1}\sum_{h|p-1}\frac{\mu(k)\mu(h)}{\phi(k)\phi(h)}\end{aligned}\tag{7}$$

$$\times \sum_{x=1}^{k}{}' \sum_{y=1}^{h}{}' \left(\sum_{a=1}^{p-1} \chi(a;x,k)\overline{\chi(a;y,h)} e\left(\frac{ra+s\overline{a}}{p}\right)\right)$$
$$\ll \frac{\phi^2(p-1)}{(p-1)^2} \sum_{k|p-1} \sum_{h|p-1} |\mu(k)| \cdot |\mu(h)| \cdot p^{\frac{1}{2}+\epsilon_1}$$
$$\ll \frac{\phi^2(p-1)}{(p-1)^2} \cdot 4^{\omega(p-1)} \cdot p^{\frac{1}{2}+\epsilon_1} \ll p^{\frac{1}{2}+\epsilon_2}$$

From (7) we have

$$(8)\quad D = \frac{1}{p^2} \sum_{r=1}^{p-1} \sum_{s=1}^{p-1} \left(\sum_{\substack{a\in\mathcal{A} \\ ab\equiv 1(p)}} \sum_{b\in\mathcal{A}} e\left(\frac{ra+sb}{p}\right)\right)$$
$$\times \left(\sum_{c=1}^{p} e\left(\frac{uc}{m} - \frac{rc}{p}\right)\right)\left(\sum_{d=1}^{p} e\left(\frac{vd}{m} - \frac{sd}{p}\right)\right)$$
$$\ll \frac{1}{p^2} \sum_{r=1}^{p-1} \sum_{s=1}^{p-1} p^{\frac{1}{2}+\epsilon_2} \cdot \min\left(p, \frac{1}{\|\frac{u}{m} - \frac{r}{p}\|}\right) \cdot \min\left(p, \frac{1}{\|\frac{v}{m} - \frac{s}{p}\|}\right)$$
$$\ll \frac{p^{\frac{1}{2}+\epsilon_2}}{p^2} \left(p + \sum_{\substack{r=1 \\ |\frac{pu}{m} - r| \geq 1}}^{p-1} \frac{p}{|\frac{pu}{m} - r|} + \sum_{\substack{r=1 \\ |\frac{(u\pm m)p}{m} - r| \geq 1}}^{p-1} \frac{p}{\left|\frac{(u\pm m)p}{m} - r\right|}\right)^2$$
$$\ll p^{\frac{1}{2}+\epsilon_2} \left(1 + \sum_{r=1}^{p-1} \frac{1}{r}\right)^2 \ll p^{\frac{1}{2}+\epsilon}$$

Combining (3), (4), (5), (6) and (8) we may immediately deduce the Lemma 3.

Lemma 4. *Let n be a positive integer with $n \geq 3$, $0 \leq \sigma \leq 1$ be any fixed positive number. Then for any fixed positive real number k, we have*

$$\sum_{\substack{a=1 \\ a=b+m}}^{n} \sum_{b=1}^{n} \sum_{m=1}^{[n\sigma]} m^k = n^{k+2} \left(\frac{\sigma^{k+1}}{k+1} - \frac{\sigma^{k+2}}{k+2}\right) + O(n^{k+1}).$$

PROOF. From Euler's summation formula we can get

$$\begin{aligned}
&\sum_{a=1}^{n}\sum_{\substack{b=1\\a=b+m}}^{n}\sum_{m=1}^{[n\sigma]} m^k = \sum_{m=1}^{[\sigma n]} m^k \sum_{b=1}^{n-m} 1\\
&= \sum_{m=1}^{[\sigma n]} m^k(n-m) = n\sum_{m=1}^{[\sigma n]} m^k - \sum_{m=1}^{[\sigma n]} m^{k+1}\\
&= n\int_0^{\sigma n} x^k dx - \int_0^{\sigma n} x^{k+1}dx + O(n^{k+1})\\
&= n\cdot\frac{\sigma^{k+1}n^{k+1}}{k+1} - \frac{\sigma^{k+1}n^{k+2}}{k+2} + O(n^{k+1})\\
&= n^{k+2}\left(\frac{\sigma^{k+1}}{k+1} - \frac{\sigma^{k+2}}{k+2}\right) + O(n^{k+1}).
\end{aligned}$$

This completes the proof of Lemma 4.

3. Proof of the theorems

From the several lemmas on the above section, we can easily deduce the proof of the theorems. In fact applying Lemma 3 and Lemma 4, and note that the trigonometric identity (2) we may get

$$\begin{aligned}
(9)\qquad M(p,k,\sigma) &= \sum_{\substack{a\in\mathcal{A}\\ab\equiv 1(p)\\|a-b|<\sigma p}}\sum_{b\in\mathcal{A}} |a-b|^k = 2\sum_{w=1}^{[\sigma p]}\sum_{\substack{a\in\mathcal{A}\\ab\equiv 1(p)\\a=b+w}}\sum_{b\in\mathcal{A}} w^k\\
&= 2\sum_{w=1}^{[\sigma p]}\sum_{\substack{a\in\mathcal{A}\\ab\equiv 1(p)}}\sum_{b\in\mathcal{A}} w^k\cdot\frac{1}{2p}\sum_{u=1}^{2p} e\left(\frac{u(a-b-w)}{2p}\right)\\
&= \frac{1}{p}\sum_{w=1}^{[\sigma p]} w^k \sum_{\substack{a\in\mathcal{A}\\ab\equiv 1(p)}}\sum_{b\in\mathcal{A}} 1 + \frac{1}{p}\sum_{u=1}^{2p-1}\left(\sum_{w=1}^{[\sigma p]} w^k e\left(\frac{-uw}{2p}\right)\right)\\
&\quad\times\left(\sum_{\substack{a\in\mathcal{A}\\ab\equiv 1(p)}}\sum_{b\in\mathcal{A}} e\left(\frac{u(a-b)}{2p}\right)\right)
\end{aligned}$$

$$= \frac{\phi(p-1)}{p}\sum_{w=1}^{[\sigma p]} w^k + \frac{1}{p}\sum_{u=1}^{2p-1}\left(\sum_{w=1}^{[\sigma p]} w^k e\left(\frac{-uw}{2p}\right)\right)$$
$$\times\left(\frac{\phi(p-1)}{p^2}\left|\sum_{c=1}^{p} e\left(\frac{uc}{2p}\right)\right|^2 + O\left(p^{\frac{1}{2}+\varepsilon}\right)\right)$$
$$= \frac{\phi(p-1)}{p}\sum_{w=1}^{[\sigma p]} w^k + \frac{\phi(p-1)}{p^3}\sum_{u=1}^{2p-1}\left(\sum_{w=1}^{[\sigma p]} w^k e\left(\frac{-uw}{2p}\right)\right)$$
$$\times\left|\sum_{c=1}^{p} e\left(\frac{uc}{2p}\right)\right|^2 + O\left(\frac{p^{\frac{1}{2}+\varepsilon}}{p}\sum_{u=1}^{2p-1}\left|\sum_{w=1}^{[\sigma p]} w^k e\left(\frac{-uw}{2p}\right)\right|\right)$$

where we have used Lemma 3 with $m = 2p$, $v = -u$.

Note that

$$\frac{\phi(p-1)}{p}\sum_{w=1}^{[\sigma p]} w^k + \frac{\phi(p-1)}{p^3}\sum_{u=1}^{2p-1}\left(\sum_{w=1}^{[\sigma p]} w^k e\left(\frac{-uw}{2p}\right)\right) \tag{10}$$
$$\times\left|\sum_{c=1}^{p} e\left(\frac{uc}{2p}\right)\right|^2$$
$$= \frac{\phi(p-1)}{p^3}\sum_{w=1}^{[\sigma p]} w^k \sum_{a=1}^{p}\sum_{b=1}^{p}\sum_{u=1}^{2p} e\left(\frac{u(a-b-w)}{2p}\right)$$
$$= \frac{2\phi(p-1)}{p^2}\sum_{a=1}^{p}\sum_{\substack{b=1\\ a=b+w}}^{p}\sum_{w=1}^{[\sigma p]} w^k$$
$$= \frac{2\phi(p-1)}{p^2}\left[p^{k+2}\left(\frac{\sigma^{k+1}}{k+1} - \frac{\sigma^{k+2}}{k+2}\right) + O(p^{k+1})\right]$$
$$= \phi(p-1)p^k\left(\frac{2\sigma^{k+1}}{k+1} - \frac{2\sigma^{k+2}}{k+2}\right) + O(p^k)$$

$$\sum_{u=1}^{2p-1}\left|\sum_{w=1}^{[\sigma p]} w^k e\left(\frac{-uw}{2p}\right)\right| \ll \sum_{u=1}^{2p-1}\frac{p^k}{\left|\sin\left(\frac{\pi u}{2p}\right)\right|} \tag{11}$$

$$\ll \sum_{u=1}^{2p-1} \frac{p^{k+1}}{u} \ll p^{k+1} \ln p.$$

Combining (9), (10) and (11) we may immediately deduce that

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

This completes the proof of the Theorem 1.

Taking $k = 0$ in Theorem 1, we can obtain Corollary 1. Similarly, taking $\sigma = 1$ in Theorem 1, we may get Corollary 2. Now we prove the Theorem 2. Note that the trigonometric identity (2), applying Lemma 3 we can obtain

$$\begin{aligned}
&\#\{a : a \in \mathcal{A},\ \overline{a} \in \mathcal{A},\ a\overline{a} \equiv 1 \pmod p,\ a \equiv \overline{a} \pmod m\} \\
&= \sum_{\substack{a\in\mathcal{A} \\ ab\equiv 1(p) \\ a\equiv b(m)}} \sum_{b\in\mathcal{A}} 1 = \frac{1}{m} \sum_{\substack{a\in\mathcal{A} \\ ab\equiv 1(p)}} \sum_{b\in\mathcal{A}} \sum_{u=1}^{m} e\left(\frac{u(a-b)}{m}\right) \\
&= \frac{\phi(p-1)}{m} + \frac{1}{m} \sum_{u=1}^{m-1} \sum_{\substack{a\in\mathcal{A} \\ ab\equiv 1(p)}} \sum_{b\in\mathcal{A}} e\left(\frac{u(a-b)}{m}\right) \\
&= \frac{\phi(p-1)}{m} + \frac{1}{m} \sum_{u=1}^{m-1} \left[\frac{\phi(p-1)}{p^2} \left| \sum_{c=1}^{p} e\left(\frac{cu}{m}\right) \right|^2 + O\left(p^{\frac{1}{2}+\varepsilon}\right) \right] \\
&= \frac{\phi(p-1)}{m} + \frac{\phi(p-1)}{p^2 m} \sum_{u=1}^{m-1} \left| \sum_{c=1}^{p} e\left(\frac{cu}{m}\right) \right|^2 + O\left(p^{\frac{1}{2}+\varepsilon}\right) \\
&= \frac{\phi(p-1)}{p^2 m} \sum_{u=1}^{m} \left| \sum_{c=1}^{p} e\left(\frac{uc}{m}\right) \right|^2 + O\left(p^{\frac{1}{2}+\varepsilon}\right) \\
&= \frac{\phi(p-1)}{p^2} \sum_{\substack{c=1 \\ c\equiv d(m)}}^{p} \sum_{d=1}^{p} 1 + O\left(p^{\frac{1}{2}+\varepsilon}\right) \\
&= \frac{\phi(p-1)}{p^2} \sum_{u=0}^{m-1} \left(\sum_{\substack{c=1 \\ c\equiv u(m)}}^{p} 1 \right)^2 + O\left(p^{\frac{1}{2}+\varepsilon}\right)
\end{aligned}$$

$$= \frac{\phi(p-1)}{p^2} \sum_{u=0}^{m-1} \left(\frac{p}{m} + O(1)\right)^2 + O\left(p^{\frac{1}{2}+\varepsilon}\right)$$
$$= \frac{\phi(p-1)}{m} + O\left(p^{\frac{1}{2}+\varepsilon}\right)$$

where the O-constant does not depend on parameter m. This completes the proof of the theorems.

Acknowledgements. The author expresses his gratitude to Professor Andrew Granville and the referee for their helpful and detailed comments.

References

[1] J.-M. Deshouillers and H. Iwaniec, Kloosterman Sum and Fourier Coefficients of Cusp Forms, *Inventiones Mathematicae* **70** (1982), 219–288.

[2] S. Chowla, On Kloostermann's sum, *Norkse Vid. Selbsk. Fak. Frondheim* **40** (1967), 70–72.

[3] Wolfgang M. Schmidt, Equations over Finite Fields, Lecture Notes in Mathematics 536, *Springer-Verlag*, *Berlin*, 1976.

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

[5] Tom M. Apostol, Introduction to Analytic Number Theory, *Springer–Verlag*, *New York*, 1976.

[6] E. Bombieri, On Exponential Sums in Finite Fields, *American Journal of Mathematics* **88** (1966), 71–105.

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

WENPENG ZHANG
DEPARTMENT OF MATHEMATICS
NORTHWEST UNIVERSITY
XI'AN SHAANXI
P. R. CHINA

(Received January 2, 1996; revised July 1, 1996)