Publ. Math. Debrecen
61 / 3-4 (2002), 383–391

On the distribution of primitive roots modulo a prime

By YI YUAN (Shaanxi) and ZHANG WENPENG (Shaanxi)

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 $\bar{x}$ modulo p with $1 \leq \bar{x} \leq p-1$ such that $x\bar{x} \equiv 1 \mod p$. Let δ be a fixed positive number with $0 \leq \delta \leq 1$, $\mathcal{A}$ denotes the set of all primitive roots modulo p in interval $[1, p]$. For any fixed positive integers k and l, the main purpose of this paper is to study the asymptotic properties of the mean value

$$N(p,k,l,m,\delta) = \sum_{\substack{a \in \mathcal{A} \\ \left|\left\{\frac{a^k}{p}\right\} - \left\{\frac{\bar{a}^l}{p}\right\}\right| < \delta}} \left|\left\{\frac{a^k}{p}\right\} - \left\{\frac{\bar{a}^l}{p}\right\}\right|^m,$$

where m be any fixed non-negative real number, $\{x\}$ denotes the fractional part of x, and give an interesting asymptotic formula.

1. Introduction

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 $\bar{x}$ modulo p with $1 \leq \bar{x} \leq p-1$ such that $x\bar{x} \equiv 1 \mod p$. Let δ be a fixed positive number with $0 \leq \delta \leq 1$, $\mathcal{A} = \mathcal{A}(p)$ denotes the set of all primitive roots modulo p in interval $[1, p]$. For any fixed positive integers k and l,

Mathematics Subject Classification: 11L05.
Key words and phrases: primitive roots, trigonometric sum, asymptotic formula, mean value.
This work is supported by the Doctorate Fundation of Xi'an Jiaotong University.

we define $N(p,k,l,m,\delta)$ as follows:

$$N(p,k,l,m,\delta) = \sum_{\substack{a\in\mathcal{A} \\ \left|\left\{\frac{a^k}{p}\right\}-\left\{\frac{\bar{a}^l}{p}\right\}\right|<\delta}} \left|\left\{\frac{a^k}{p}\right\}-\left\{\frac{\bar{a}^l}{p}\right\}\right|^m \tag{1}$$

where m be any fixed non-negative real number, $\{x\} = x - [x]$ denotes the fractional part of x ($[x]$ denoting the integral part of x). The main purpose of this paper is to study the asymptotic properties of $N(p,k,l,m,\delta)$.

About this problem, the second author [3] considered the case $k = l = 1$, and obtained a sharp asymptotic formula, which reads

$$\begin{aligned} N(p,m,\delta) &= \sum_{\substack{a\in\mathcal{A} \\ |a-\bar{a}|<\delta p}} |a-\bar{a}|^m \\ &= 2\phi(p-1)p^m\left(\frac{\delta^{m+1}}{m+1}-\frac{\delta^{m+2}}{m+2}\right) + O\left(p^{m+\frac{1}{2}+\epsilon}\right), \end{aligned}$$

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

It is quite natural and interesting to consider the case of (1). In this paper, we use a trigonometric estimate and the G. I. Perel'muter's deep result to prove a sharp asymptotic formula for $N(p,k,l,m,\delta)$ in the same setting as in paper [3].

Our main result is the following:

Theorem. *Let $p \geq 3$ be a prime, δ be a fixed positive number with $0 \leq \delta \leq 1$ and m be any fixed non-negative real number. Then for any fixed positive integers k and l, we have the asymptotic formula*

$$N(p,k,l,m,\delta) = 2\phi(p-1)\left(\frac{\delta^{m+1}}{m+1}-\frac{\delta^{m+2}}{m+2}\right) + O\left(p^{\frac{1}{2}+\epsilon}\right),$$

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

For $m = 0$, from this theorem we may immediately deduce the following:

Corollary. *For any prime $p > 2$ and any fixed positive integer k and l, we have the asymptotic formula*

$$N(p,k,l,\delta) = \delta\cdot(2-\delta)\cdot\phi(p-1) + O\left(p^{\frac{1}{2}+\epsilon}\right).$$

2. Some lemmas

To complete the proof of the theorem, we need following several lemmas.

Lemma 1. *Let $p \geq 3$ be a prime, m and n be any fixed integers with $(mn, p) = 1$. Let χ denotes a Dirichlet character modulo p. Then for any fixed positive integers k and l, we have the estimate*

$$\sum_{a=1}^{p-1} \chi(a) e\left(\frac{ma^k + n\bar{a}^l}{p}\right) \ll \sqrt{p}.$$

Proof. Taking rational functions $R_1(a) = a$ and $R_2(a) = \frac{m \cdot a^{k+l} + n}{a^l}$. By Theorem 4 of [1] we may immediately obtain the estimate

$$\sum_{a=1}^{p-1} \chi(R_1(a)) e\left(\frac{R_2(a)}{p}\right) \ll \sqrt{p}.$$

This proves Lemma 1. □

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

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

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 [2].) □

Lemma 3. *Let $p \geq 3$ be a prime, r and s be integers. Then for any fixed positive integers k and l, we have the estimate*

$$\sum_{a \in \mathcal{A}} e\left(\frac{r \cdot a^k + s \cdot \bar{a}^l}{p}\right) = O\left(p^{\frac{1}{2}+\epsilon} (r, s, p)^{\frac{1}{2}}\right).$$

Proof. If $p \mid s$ and $p \mid r$, then Lemma 3 is trivial. If $p \mid r$ or $p \mid s$, but $p \nmid r+s$, then by the Gauss sum we also have the estimate of Lemma 3. So without loss of generality, we can assume $(rs,p)=1$. Then from Lemma 1 and Lemma 2 we can easily deduce that

$$\begin{aligned}
\sum_{a\in\mathcal{A}} e\left(\frac{r\cdot a^k + s\cdot \bar{a}^l}{p}\right) &= \frac{\phi^2(p-1)}{(p-1)^2}\sum_{j\mid p-1}\sum_{h\mid p-1}\frac{\mu(j)\mu(h)}{\phi(j)\phi(h)} \\
&\quad\times \sideset{}{'}\sum_{x=1}^{j}\sideset{}{'}\sum_{y=1}^{h}\sum_{a=1}^{p-1} e\left(\frac{x\operatorname{ind} a}{j}+\frac{y\operatorname{ind}\bar{a}}{h}\right) e\left(\frac{r\cdot a^k + s\cdot \bar{a}^l}{p}\right) \\
&= \frac{\phi^2(p-1)}{(p-1)^2}\sum_{j\mid p-1}\sum_{h\mid p-1}\frac{\mu(j)\mu(h)}{\phi(j)\phi(h)} \\
&\quad\times \sideset{}{'}\sum_{x=1}^{j}\sideset{}{'}\sum_{y=1}^{h}\sum_{a=1}^{p-1} \chi(a;x,j)\chi(\bar{a};y,h) e\left(\frac{r\cdot a^k + s\cdot \bar{a}^l}{p}\right) \\
&= \frac{\phi^2(p-1)}{(p-1)^2}\sum_{j\mid p-1}\sum_{h\mid p-1}\frac{\mu(j)\mu(h)}{\phi(j)\phi(h)} \\
&\quad\times \sideset{}{'}\sum_{x=1}^{j}\sideset{}{'}\sum_{y=1}^{h}\sum_{a=1}^{p-1} \chi(a;x,j)\overline{\chi(a;y,h)} e\left(\frac{r\cdot a^k + s\cdot \bar{a}^l}{p}\right) \\
&\ll \frac{\phi^2(p-1)}{(p-1)^2}\sum_{j\mid p-1}\sum_{h\mid p-1}|\mu(j)|\cdot|\mu(h)|p^{\frac{1}{2}} \\
&\ll \frac{\phi^2(p-1)}{(p-1)^2}\cdot 4^{\omega(p-1)}\cdot p^{\frac{1}{2}} \ll p^{\frac{1}{2}+\epsilon},
\end{aligned}$$

where $\chi(a;x,j)=e\left(\frac{x\operatorname{ind} a}{j}\right)$ denotes a Dirichlet character modulo p, $\omega(n)$ denotes the number of all different prime divisors of n, ϵ is any fixed positive number, $\sideset{}{'}\sum_{x=1}^{j}$ denotes the summation over all $1\le x\le j$ with $(x,j)=1$.

This proves Lemma 3. □

Lemma 4. *Let $p \geq 3$ be a prime, m be any fixed non-negative real number. Then for any fixed real number $0 \leq \delta \leq 1$, we have the estimate*

$$\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left|\sum_{\substack{c=1\\|c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1}|c-d|^m e\left(\frac{-rc-sd}{p}\right)\right| = O\left(p^{2+m}\ln^2 p\right).$$

Proof. First note the trigonometric identity

$$\sum_{a=1}^{n} e(ax) = e\left(\frac{(n+1)x}{2}\right)\frac{\sin \pi n x}{\sin \pi x}. \tag{2}$$

So from (2) we obtain

$$\begin{aligned}
&\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left|\sum_{\substack{c=1\\|c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1}|c-d|^m e\left(\frac{-rc-sd}{p}\right)\right| \\
&\ll \sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left|\sum_{w=0}^{[\delta p]} w^m \sum_{\substack{c=1\\c-d=w}}^{p-1}\sum_{d=1}^{p-1} e\left(\frac{-rc-sd}{p}\right)\right| \\
&\ll \sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left|\sum_{w=0}^{[\delta p]} w^m \sum_{d=1}^{p-1-w} e\left(\frac{-r(d+w)-sd}{p}\right)\right| \\
&\ll \sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left|\sum_{w=0}^{[\delta p]} w^m \cdot e\left(\frac{-rw}{p}\right)\sum_{d=1}^{p-1-w} e\left(\frac{-(r+s)d}{p}\right)\right| \\
&\ll \sum_{r=1}^{p-1}\left|\sum_{w=0}^{[\delta p]} w^m \cdot e\left(\frac{-rw}{p}\right)\cdot(p-1-w)\right| \\
&\quad + \sum_{\substack{r=1\\r+s\neq p}}^{p-1}\sum_{s=1}^{p-1}\left|\sum_{w=0}^{[\delta p]} w^m \cdot e\left(\frac{-rw}{p}\right)\cdot e\left(\frac{-(r+s)}{p}\right)\right. \\
&\quad \left.\cdot \frac{e\left(\frac{-(r+s)(p-1-w)}{p}\right)-1}{e\left(\frac{-(r+s)}{p}\right)-1}\right|
\end{aligned} \tag{3}$$

$$\ll \sum_{r=1}^{p-1}\left|\sum_{w=0}^{[\delta p]} w^m e\left(\frac{-rw}{p}\right)\cdot(p-1-w)\right| + \sum_{\substack{r=1\\ r+s\neq p}}^{p-1}\sum_{s=1}^{p-1}\frac{1}{\left|e\left(\frac{-(r+s)}{p}\right)-1\right|}$$

$$\times\left|\sum_{w=0}^{[\delta p]} w^m e\left(\frac{-rw-(r+s)(p-1-w)}{p}\right) - \sum_{w=0}^{[\delta p]} w^m\cdot e\left(\frac{-rw}{p}\right)\right|.$$

Noting that the trigonometric estimate

$$\sum_{m\leq M} m^k e(mx) \leq M^k\cdot\min\left(M, \frac{1}{|\sin \pi x|}\right), \qquad \text{if } k\geq 0. \tag{4}$$

From (3) and (4) we immediately get

$$\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left|\sum_{\substack{c=1\\ |c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1}|c-d|^m e\left(\frac{-rc-sd}{p}\right)\right|$$

$$\ll \sum_{r=1}^{p-1}\frac{p^{m+1}}{\left|\sin\frac{\pi r}{p}\right|} + \sum_{\substack{r=1\\ r+s\neq p}}^{p-1}\sum_{s=1}^{p-1}\frac{1}{\left|\sin\frac{\pi(r+s)}{p}\right|}\left[\frac{p^m}{\left|\sin\frac{\pi r}{p}\right|}+\frac{p^m}{\left|\sin\frac{\pi s}{p}\right|}\right]$$

$$\ll p^{2+m}\ln p + p^m\cdot\sum_{r=1}^{p-1}\frac{1}{\left|\sin\frac{\pi r}{p}\right|}\sum_{\substack{s=1\\ s\neq p-r}}^{p-1}\frac{1}{\left|\sin\frac{\pi(r+s)}{p}\right|}$$

$$\ll p^{2+m}\ln^2 p.$$

This proves Lemma 4. □

3. Proof of the theorem

In this section, we complete the proof of the Theorem. First note the trigonometric identity

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

and the identity

$$\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left(\sum_{a\in\mathcal{A}} e\left(\frac{r\cdot p\left\{\frac{a^k}{p}\right\}+s\cdot p\left\{\frac{\bar{a}^l}{p}\right\}}{p}\right)\right)$$
$$=\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left(\sum_{a\in\mathcal{A}} e\left(\frac{r\cdot a^k+s\cdot \bar{a}^l}{p}\right)\right).$$

From these trigonometric identities, Lemma 3 and Lemma 4, we have

$$N(p,k,l,m,\delta)=\sum_{\substack{a\in\mathcal{A}\\ \left|\left\{\frac{a^k}{p}\right\}-\left\{\frac{\bar{a}^l}{p}\right\}\right|<\delta}}\left|\{\frac{a^k}{p}\}-\{\frac{\bar{a}^l}{p}\}\right|^m$$

$$=\frac{1}{p^2}\sum_{r,s=1}^{p}\sum_{a\in\mathcal{A}}\sum_{\substack{c=1\\ |c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1}\frac{1}{p^m}|c-d|^m e\left(\frac{r\left(p\left\{\frac{a^k}{p}\right\}-c\right)}{p}\right)e\left(\frac{s\left(p\left\{\frac{\bar{a}^l}{p}\right\}-d\right)}{p}\right)$$

$$=\frac{1}{p^{2+m}}\sum_{r,s=1}^{p}\left(\sum_{a\in\mathcal{A}} e\left(\frac{r\cdot p\left\{\frac{a^k}{p}\right\}+s\cdot p\left\{\frac{\bar{a}^l}{p}\right\}}{p}\right)\right)$$
$$\times\sum_{\substack{c=1\\ |c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1}|c-d|^m e\left(\frac{-rc-sd}{p}\right)$$

$$=\frac{1}{p^{2+m}}\sum_{r,s=1}^{p}\left(\sum_{a\in\mathcal{A}} e\left(\frac{r\cdot a^k+s\cdot\bar{a}^l}{p}\right)\right)\sum_{\substack{c=1\\ |c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1}|c-d|^m e\left(\frac{-rc-sd}{p}\right)$$

$$=\frac{1}{p^{2+m}}\sum_{a\in\mathcal{A}}\sum_{\substack{c=1\\ |c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1}|c-d|^m$$
$$+\frac{1}{p^{2+m}}\sum_{r=1}^{p-1}\left(\sum_{a\in\mathcal{A}} e\left(\frac{r\cdot a^k}{p}\right)\right)\cdot\sum_{\substack{c=1\\ |c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1}|c-d|^m e\left(\frac{-rc}{p}\right)$$

$$
\begin{aligned}
&+\frac{1}{p^{2+m}}\sum_{s=1}^{p-1}\left(\sum_{a\in\mathcal{A}}e\left(\frac{s\cdot\bar{a}^l}{p}\right)\right)\cdot\sum_{\substack{c=1\\|c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1}|c-d|^m e\left(\frac{-sd}{p}\right)\\
&+\frac{1}{p^{2+m}}\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left(\sum_{a\in\mathcal{A}}e\left(\frac{r\cdot a^k+s\cdot\bar{a}^l}{p}\right)\right)\\
&\times\sum_{\substack{c=1\\|c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1}|c-d|^m e\left(\frac{-rc-sd}{p}\right)\\
=&\frac{1}{p^{2+m}}\cdot\phi(p-1)\left(2\cdot\sum_{w=0}^{[\delta p]}\sum_{\substack{c=1\\c-d=w}}^{p-1}\sum_{d=1}^{p-1}w^m\right)+O(1)\\
&+O\left(p^{-2-m+\frac{1}{2}+\epsilon}\cdot\sum_{r=1}^{p-1}\left|\sum_{\substack{c=1\\|c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1}|c-d|^m e\left(\frac{-rc}{p}\right)\right|\right)\\
&+O\left(p^{-2-m+\frac{1}{2}+\epsilon}\cdot\sum_{r=1}^{p-1}\sum_{s=1}^{p-1}\left|\sum_{\substack{c=1\\|c-d|<\delta p}}^{p-1}\sum_{d=1}^{p-1}|c-d|^m e\left(\frac{-rc-sd}{p}\right)\right|\right)\\
=&\frac{1}{p^{2+m}}\cdot\phi(p-1)\left(2\cdot\sum_{w=0}^{[\delta p]}w^m\cdot(p-1-w)\right)+O(1)\\
&+O\left(p^{-2+\frac{1}{2}+\epsilon}\cdot\sum_{c=1}^{p-1}(\delta p+c)\cdot\frac{1}{\left|\sin\frac{\pi c}{p}\right|}\right)+O\left(p^{\frac{1}{2}+\epsilon}\right)\\
=&\frac{2}{p^{2+m}}\cdot\phi(p-1)\left(\frac{\delta^{m+1}p^{m+2}}{m+1}-\frac{\delta^{m+2}p^{m+2}}{m+2}+O(p^{m+1})\right)+O\left(p^{\frac{1}{2}+\epsilon}\right)\\
=&2\cdot\phi(p-1)\left(\frac{\delta^{m+1}}{m+1}-\frac{\delta^{m+2}}{m+2}\right)+O\left(p^{\frac{1}{2}+\epsilon}\right).
\end{aligned}
$$

This completes the proof of Theorem.

Acknowledgement. The authors express their gratitude to the referee for his helpful and detailed comments.

References

[1] G. I. Perel'muter, On certain character sums, *Uspehi Mat. Nauk* **18** (1963), 145–149. (in *Russian*)

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

[3] Zhang Wenpeng, On the distribution of primitive roots modulo p, *Publicationes Mathematicae Debrecen* **53** (1998), 245–255.

YI YUAN
RESEARCH CENTER FOR BASIC SCIENCE
XI'AN JIAOTONG UNIVERSITY
XI'AN
P.R. CHINA

ZHANG WENPENG
RESEARCH CENTER FOR BASIC SCIENCE
XI'AN JIAOTONG UNIVERSITY
XI'AN
P.R. CHINA

(Received May 28, 2001; revised May 8, 2002)