文章编号: 1000-341X(2007)02-0403-05 **文献标识码**: A

关于模 p^α 原根分布的推广

钱 淼 岚
(复旦大学数学所, 上海 200433)
(E-mail: annaqml@yahoo.com.cn)

摘 要: 设 p 为奇素数, α 为任意大于 1 的整数, 对于任意给定的正整数 k, $k|p^\alpha - p^{\alpha-1}$, 本文主要研究模 p^α 的 k 次剩余的分布性质.

关键词: 原根; 三角和; Kloostermann 和.
MSC(2000): 11A07; 11L05; 11N69
中图分类: O156.4

1 引 言

设 p 为奇素数, g 是模 p 的一个原根, 则存在一个整数 t_0, 使得由等式 $(g+pt_0)^{p-1} = 1+pu_0$ 所确定的 u_0 不能被 p 整除, 并且对应这个 t_0 的 $g+pt_0$ 就是模 p^α 的原根, 其中 α 是大于 1 的任意整数. 由欧拉定理: 设 m 是大于 1 的整数, $(a,m)=1$, 则 $a^{\varphi(m)} \equiv 1 \pmod m$. 对于模 p^α 的任一满足 $1 \le x \le p^\alpha - 1$ 的原根 x, 一定存在模 p^α 唯一的原根 $\bar{x}$ 满足 $1 \le \bar{x} \le p^\alpha - 1$, 且 $x\bar{x} \equiv 1 \pmod{p^\alpha}$. 对于任意给定的正整数 k, $k|p^\alpha - p^{\alpha-1}$ 及任意给定的实数 $0 < \delta < 1$, 设 A 表示区间 $[1, p^\alpha]$ 内模 p^α 的所有原根之集.

本文对文献 [1] 中的结论给予推广, 即研究了对任意给定的正整数 $\alpha > 1$, $\sum\limits_{\substack{a\in A\\ |\{\frac{ak}{p^\alpha}\}-\{\frac{\bar{a}k}{p^\alpha}\}|<\delta}} 1$ 的渐近性质.

2 主要结果

定理 设 p 为奇素数, 对于任意给定的正整数 k, $k|p^\alpha - p^{\alpha-1}$ 及实数 $0 < \delta < 1$, 则有渐近公式

$$\sum_{\substack{a\in A\\ |\{\frac{ak}{p^\alpha}\}-\{\frac{\bar{a}k}{p^\alpha}\}|<\delta}} 1 = \varphi(p^\alpha - p^{\alpha-1})\delta(2-\delta) + O(p^{\alpha-\frac{1}{4}+\varepsilon}),$$

其中 $\varphi(n)$ 为欧拉函数, ε 为任意给定的正数, $\{x\} = x - [x]$, $[x]$ 表示不超过 x 的最大整数.

由上述定理, 容易得到以下推论.

推论 设 p 为奇素数, 则对任意给定的实数 $0 < \delta < 1$, 有极限分布

$$\lim_{p\to+\infty} \frac{1}{\varphi(p^\alpha - p^{\alpha-1})} \sum_{\substack{a\in A\\ |\{\frac{ak}{p^\alpha}\}-\{\frac{\bar{a}k}{p^\alpha}\}|<\delta}} 1 = \delta(2-\delta).$$

收稿日期: 2004-01-20; **接受日期**: 2004-05-01

在证明上述结论之前，首先介绍证明中需要用到的几个引理.

引理 1 设 m,n 及 q 是整数且 $q \geq 2$, 则有估计式

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

其中 $d\bar{d} \equiv 1 \pmod q$, $\sum_d{}'$ 表示所有满足 $(d,q)=1$ 的 d 求和，$d(q)$ 为除数函数，$e(y)=e^{2\pi iy}$, (m,n,q) 表示 m, n 及 q 的最大公因子.

证明 参见文献 [2].

引理 2 设 p 为奇素数，m, n 为整数，χ 表示模 p 的任一 Dirichlet 特征，则对任意给定的正整数 $k|p-1$, 有估计式

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

证明 参见文献 [3].

引理 3 设 p 为奇素数，m, n 为整数，χ 表示模 p^α 的任一 Dirichlet 特征，则对任意给定的正整数 k, $k|p^\alpha-p^{\alpha-1}$, 有估计式

$$\sum_{a=1}^{p^\alpha-1}\chi(a)e(\frac{ma^k+n\bar{a}^k}{p^\alpha}) \ll p^{\frac{3}{4}\alpha}(m,n,p)^{\frac{1}{4}}.$$

证明 p 为奇素数，a 与 p^α 不互素时，不必考虑；a 与 p^α 互素时，则一定存在 $\bar{a}$ ($\bar{a}$ 可取为 $as+p^\alpha t=1$ 中 s 的剩余类代表). 对任意给定的正整数 k, $k|p^\alpha-p^{\alpha-1}$ 有恒等式

$$\begin{aligned}|\sum_{a=1}^{p^\alpha-1}\chi(a)e(\frac{ma^k+n\bar{a}^k}{p^\alpha})|^2 &= \sum_{a=1}^{p^\alpha-1}\sum_{b=1}^{p^\alpha-1}\chi(a\bar{b})e(\frac{m(a^k-b^k)+n(\bar{a}^k-\bar{b}^k)}{p^\alpha})\\ &=(p^{\alpha-1})\sum_{r=0}^{k-1}\chi(g^{\frac{r(p^\alpha-p^{\alpha-1})}{k}})+\\ &\quad\sum_{\substack{a=1\\ a^k\not\equiv 1 \pmod{p^\alpha}}}^{p^\alpha-1}\chi(a)\sum_{l=1}^{p^\alpha-p^{\alpha-1}-1}e(\frac{mg^{kl}(a^k-1)+n\bar{g}^{kl}(\bar{a}^k-1)}{p^\alpha}),\end{aligned}$$

其中，g 为模 p^α 任意给定的原根. 对于任一整数 r, $0 \leq r \leq k-1$, 有恒等式

$$\begin{aligned}&|\sum_{a=1}^{p^\alpha-1}\chi(a)e(\frac{mg^ra^k+n\bar{g}^r\bar{a}^k}{p^\alpha})|^2\\ &=\sum_{\substack{a=1\\ a^k\not\equiv 1 \pmod{p^\alpha}}}^{p^\alpha-1}\chi(a)\sum_{l=0}^{p^\alpha-p^{\alpha-1}-1}e(\frac{mg^{kl+r}(a^k-1)+n\bar{g}^{kl+r}(\bar{a}^k-1)}{p^\alpha})+(p^{\alpha-1})\sum_{r=0}^{k-1}\chi(g^{\frac{r(p^\alpha-p^{\alpha-1})}{k}}).\end{aligned}$$

同时注意到如果 r 通过 0 到 $k-1$ 且 l 通过 0 到 $p^\alpha-p^{\alpha-1}-1$, 那么 g^{kl+r} 通过模 p^α 的 k 个简化剩余系. b 与 p^α 互素，则 $\bar{b}$ 与 p^α 互素. a^k-1 与 p^α 不互素，则 $\bar{a}^k-1$ 与 p^α 也不互素，

且两者与 p^α 公因子相同. 因此，由上述两式及引理 1 可得

$$\begin{aligned}
|\sum_{a=1}^{p^\alpha-1}\chi(a)e(\frac{ma^k+n\bar{a}^k}{p^\alpha})|^2 \le & \sum_{r=0}^{k-1}|\sum_{a=1}^{p^\alpha-1}\chi(a)e(\frac{mg^ra^k+n\bar{g}^r\bar{a}^k}{p^\alpha})|^2\\
= & \sum_{\substack{a=1\\ a^k\not\equiv 1 \pmod{p^\alpha}}}^{p^\alpha-1}\chi(a)\sum_{r=0}^{k-1}\sum_{l=0}^{p^\alpha-p^{\alpha-1}-1}e(\frac{mg^{kl+r}(a^k-1)+n\bar{g}^{kl+r}(\bar{a}^k-1)}{p^\alpha})+\\
& k(p^{\alpha-1})\sum_{r=0}^{k-1}\chi(g^{\frac{r(p^\alpha-p^{\alpha-1})}{k}})\\
\le & k(p^\alpha-1)\sum_{r=0}^{k-1}\chi(g^{\frac{r(p^\alpha-p^{\alpha-1})}{k}})+\\
& \sum_{s=0}^{\alpha-1}k\sum_{\substack{a=1\\ a^k\not\equiv 1 \pmod{p^\alpha}\\ (a^k-1,p^\alpha)=p^s}}^{p^\alpha-1}\chi(a)\sum_{b=1}^{p^\alpha-1}e(\frac{mb(a^k-1)+n\bar{b}(\bar{a}^k-1)}{p^\alpha})\\
\ll & k^2(p^\alpha-1)+\sum_{s=0}^{\alpha-1}k\sum_{\substack{a=1\\ a^k\not\equiv 1 \pmod{p^\alpha}\\ (a^k-1,p^\alpha)=p^s}}^{p^\alpha-1}p^{\frac{1}{2}s}(m,n,p^s)^{\frac{1}{2}}d(p^s)\\
\ll & k^2(p^\alpha-1)+\sum_{s=0}^{\alpha-1}k\sum_{\substack{a=1\\ a^k\not\equiv 1 \pmod{p^\alpha}\\ (a^k-1,p^\alpha)=p^s}}^{p^\alpha-1}p^{\frac{1}{2}s}(m,n,p^s)^{\frac{1}{2}}(s+1)\\
\ll & p^{\frac{3}{2}\alpha}(m,n,p^s)^{\frac{1}{2}}.
\end{aligned}$$

这样引理 3 成立.

引理 4 设模 $n\ge 3$ 且存在一个原根，则对任一满足 $(m,n)=1$ 的整数 m, 有恒等式

$$\sum_{k|\varphi(n)}\frac{\mu(k)}{\varphi(k)}\sum_{\substack{a=1\\ (a,k)=1}}^{k}e(\frac{a\ \mathrm{ind}\, m}{k})=\begin{cases}\frac{\varphi(n)}{\varphi(\varphi(n))}, & \text{如果 } m \text{ 是模 } n \text{ 的一个原根;}\\ 0, & \text{其他.}\end{cases}$$

式中 $\mu(n)$ 为 Möbius 函数， $\mathrm{ind}\, m$ 表示 m 相对于模 n 的任一给定原根的指标.

证明 参见文献 [4].

引理 5 设 $p\ge 3$ 为素数， r,s 为整数，则对任意给定的整数 $k|p^\alpha-p^{\alpha-1}$, 有估计式

$$\sum_{\substack{a\in A b\in A\\ ab\equiv 1 \pmod{p^\alpha}}}\sum e(\frac{r\cdot a^k+s\cdot b^k}{p^\alpha})=O(p^{\frac{3}{4}\alpha+\varepsilon}(r,s,p^\alpha)^{\frac{1}{4}}).$$

证明 当文献 [1] 方法中的 $p-1$ 处由 $p^\alpha-p^{\alpha-1}$ 代替，则此结果可由文献 [1] 及初等方法容易证明，故略.

引理 6 设 p 为奇素数，则对任意给定的实数 $0<\delta<1$, 有估计式

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

证明 当文献 [1] 方法中的 p 处由 p^α 代替, 则此结果亦可由文献 [1] 及初等方法容易证明, 故略.

3 定理证明

利用三角恒等式

$$\sum_{r=1}^{q} e(\frac{rn}{q}) = \begin{cases} q, \text{ 如果 } q|n \\ 0, \text{ 如果 } q \not| n \end{cases}$$

以及恒等式

$$\sum_{r=1}^{p^\alpha-1}\sum_{s=1}^{p^\alpha-1}\Big[\sum_{\substack{a\in A b\in A\\ ab\equiv 1 \pmod{p^\alpha}}}\sum e(\frac{rp^\alpha\{\frac{a^k}{p^\alpha}\}+sp^\alpha\{\frac{b^k}{p^\alpha}\}}{p^\alpha})\Big] = \sum_{r=1}^{p^\alpha-1}\sum_{s=1}^{p^\alpha-1}\Big[\sum_{a\in A} e(\frac{ra^k+s\bar{a}^k}{p^\alpha})\Big].$$

应用三角和估计, 及前述引理有

$$\begin{aligned}
\sum_{\substack{a\in A\\ |\{\frac{ak}{p^\alpha}\}-\{\frac{\bar{a}k}{p^\alpha}\}|<\delta}} 1 =& \sum_{\substack{a\in A\\ ab\equiv 1 \pmod{p^\alpha}\\ |\{\frac{ak}{p^\alpha}\}-\{\frac{bk}{p^\alpha}\}|<\delta}}\sum_{b\in A} 1\\
=& \frac{1}{p^{2\alpha}}\sum_{r,s=1}^{p^\alpha}\sum_{\substack{a\in A b\in A\\ ab\equiv 1 \pmod{p^\alpha}}}\sum \sum_{\substack{c=1\\ |c-d|<\delta p^\alpha}}^{p^\alpha-1}\sum_{d=1}^{p^\alpha-1} e\Big(\frac{r(p^\alpha\{\frac{a^k}{p^\alpha}\}-c)}{p^\alpha}\Big)e\Big(\frac{s(p^\alpha\{\frac{b^k}{p^\alpha}\}-d)}{p^\alpha}\Big)\\
=& \frac{1}{p^{2\alpha}}\sum_{r,s=1}^{p^\alpha}\Big[\sum_{\substack{a\in A b\in A\\ ab\equiv 1 \pmod{p^\alpha}}}\sum e\Big(\frac{rp^\alpha\{\frac{a^k}{p^\alpha}\}+sp^\alpha\{\frac{b^k}{p^\alpha}\}}{p^\alpha}\Big)\Big]\sum_{\substack{c=1\\ |c-d|<\delta p^\alpha}}^{p^\alpha-1}\sum_{d=1}^{p^\alpha-1} e\Big(\frac{-rc-sd}{p^\alpha}\Big)\\
=& \frac{1}{p^{2\alpha}}\sum_{r,s=1}^{p^\alpha}\Big[\sum_{\substack{a\in A b\in A\\ ab\equiv 1 \pmod{p^\alpha}}}\sum e(\frac{ra^k+sb^k}{p^\alpha})\Big]\sum_{\substack{c=1\\ |c-d|<\delta p^\alpha}}^{p^\alpha-1}\sum_{d=1}^{p^\alpha-1} e\Big(\frac{-rc-sd}{p^\alpha}\Big)\\
=& \frac{1}{p^{2\alpha}}\sum_{\substack{a\in A b\in A\\ ab\equiv 1 \pmod{p^\alpha}}}\sum \sum_{\substack{c=1\\ |c-d|<\delta p^\alpha}}^{p^\alpha-1}\sum_{d=1}^{p^\alpha-1} 1+\frac{2}{p^{2\alpha}}\sum_{r=1}^{p^\alpha}\Big[\sum_{a\in A} e(\frac{ra^k}{p^\alpha})\Big]\sum_{\substack{c=1\\ |c-d|<\delta p^\alpha}}^{p^\alpha-1}\sum_{d=1}^{p^\alpha-1} e(\frac{-rc}{p^\alpha})+\\
& \frac{1}{p^{2\alpha}}\sum_{r=1}^{p^\alpha}\sum_{s=1}^{p^\alpha}\Big[\sum_{\substack{a\in A b\in A\\ ab\equiv 1 \pmod{p^\alpha}}}\sum e(\frac{ra^k+sb^k}{p^\alpha})\Big]\sum_{\substack{c=1\\ |c-d|<\delta p^\alpha}}^{p^\alpha-1}\sum_{d=1}^{p^\alpha-1} e(\frac{-rc-sd}{p^\alpha})\\
=& \frac{1}{p^{2\alpha}}\varphi(p^\alpha-p^{\alpha-1})\Big[2\sum_{m=0}^{[\delta p^\alpha]}\sum_{\substack{c=1\\ c-d=m}}^{p^\alpha-1}\sum_{d=1}^{p^\alpha-1} 1\Big]+O(1)+\\
& O\Big(p^{(-2+\frac{3}{4})\alpha+\varepsilon}(r,s,p^\alpha)^{\frac{1}{4}}\sum_{r=1}^{p^\alpha-1}\Big|\sum_{\substack{c=1\\ |c-d|<\delta p^\alpha}}^{p^\alpha-1}\sum_{d=1}^{p^\alpha-1} e(\frac{-rc}{p^\alpha})\Big|\Big)+\\
& O\Big(p^{(-2+\frac{3}{4})\alpha+\varepsilon}(r,s,p^\alpha)^{\frac{1}{4}}\sum_{r=1}^{p^\alpha-1}\sum_{s=1}^{p^\alpha-1}\Big|\sum_{\substack{c=1\\ |c-d|<\delta p^\alpha}}^{p^\alpha-1}\sum_{d=1}^{p^\alpha-1} e(\frac{-rc-sd}{p^\alpha})\Big|\Big)
\end{aligned}$$

$$
\begin{aligned}
=&\frac{1}{p^{2\alpha}}\varphi(p^\alpha-p^{\alpha-1})\Big[2\sum_{m=0}^{[\delta p^\alpha]}(p^\alpha-1-m)\Big]+O(1)+\\
&O\Big(p^{(-2+\frac{3}{4})\alpha+\varepsilon}(r,s,p^\alpha)^{\frac{1}{4}}\sum_{c=1}^{p^\alpha-1}(\delta p^\alpha+c)\frac{1}{|\sin\frac{\pi c}{p^\alpha}|}\Big)+O\Big(p^{\frac{3}{4}\alpha+\varepsilon}(r,s,p^\alpha)^{\frac{1}{4}}\Big)\\
=&\frac{1}{p^{2\alpha}}\varphi(p^\alpha-p^{\alpha-1})\Big[2p^\alpha(\delta p^\alpha+1)-\delta^2p^{2\alpha}+O(p^\alpha)\Big]+O(p^{\alpha-\frac{1}{4}+\varepsilon})\\
=&\varphi(p^\alpha-p^{\alpha-1})\delta(2-\delta)+O(p^{\alpha-\frac{1}{4}+\varepsilon}).
\end{aligned}
$$

这样就得到 α 为任意大于 1 的整数，对于任意给定的正整数 $k|p^\alpha-p^{\alpha-1}$, 模 p^α 的 k 次剩余的分布性质.

参考文献:

[1] YI Yuan, ZHANG Wen-peng. *On the distribution of primitive roots modulo p* [J]. J. Ningxia Univ. Nat. Sci. Ed., 2002, **23**(1): 6–8.
[2] APOSTOL T M. *Introduction to Analytic Number Theory* [M]. Springer-Verlag, 1976.
[3] CHOWLA S. *On Kloostermann's sun* [J]. Norske Vid. Selsk. Forh. (Trondheim), 1967, **40**: 70–72.
[4] NARKIEWICZ W. *Classical Problems in Number Theory* [M]. PWN-Polish Scientific Publishers, 1987.

Extension on the Distribution of Primitive Roots Modulo p

QIAN Miao-lan
(Department of Mathematics, Fudan University, Shanghai 200433, China)

Abstract: Let p be an odd prime. k is a positive integer with $k|p^\alpha-p^{\alpha-1}$. The main purpose of this paper is to study the distribution of k-th residue modulo p^α, when α is a positive integer with $\alpha>1$.

Key words: primitive root; trigonometric sums; Kloostermann sum.