第18卷第4期 数学研究与评论 Vol. 18 No. 4
1998年11月 JOURNAL OF MATHEMATICAL RESEARCH AND EXPOSITION Nov. 1998

关于模N 的原根与它的逆的差的奇数幂及其推广*

王 辉[1] 王世勤[2] 胡志兴[3] 高 丽[1]

([1]延安大学数学系, 延安716000)

([2]延安农校, 延安716000)

([3]北京航空航天大学数理系, 北京100083)

摘 要 本文研究了模 n 的原根 a 与它的逆 $\bar{a}$ 差的奇数幂分布性质, 并给出了 $\sum_{\substack{a\le xn\\ \bar{a}\le yn\\ a\in A}} |a-\bar{a}|^{2k+1}$ 的一个渐近公式

关键词 原根, 逆, 分布性质, 渐近公式。

分类号 AMS(1991) 11L05/CCL O156.4

1 引 言

设整数 $n\ge 3$, 对任一整数 $1\le a\le n-1$ 且 $(a,n)=1$, 显然存在唯一整数 $1\le \bar{a}\le n-1$ 使得 $a\bar{a}\equiv 1 (\mathrm{mod} n)$, 把满足这一同余方程的 $\bar{a}$ 称为 a 模 n 的逆. 若 $n\ge 3$ 存在原根, 设 A 表示区间 $[1,n]$ 中模 n 的所有原根之集合, 本文将借助于Weil 关于 Kloosterman 和估计及三角和方法来研究模 n 的原根与它的逆的差的奇数幂的分布性质及其推广, 即研究 $\sum_{\substack{a\le xn\\ \bar{a}\le yn\\ a\in A}} |a-\bar{a}|^{2k+1}$ 的渐近性质, 其中 k 为非负整数, 实数 $0<x,y\le 1$. 证明了下面的结论:

定理 设模 $n\ge 3$ 存在原根, 对非负整数 k 和实数 $0<x,y\le 1$, 有渐近公式

$$\sum_{\substack{a\le xn\\ \bar{a}\le yn\\ a\in A}} |a-\bar{a}|^{2k+1}=\frac{\varphi(\varphi(n))n^{2k+1}}{(2k+3)(k+2)}\left(x^{2k+4}+y^{2k+4}-(x-y)^{2k+4}\right)+$$

$$O\left(4^k n^{2k+\frac{3}{2}} d^2(n) 4^{\omega(\varphi(n))}\ln^4 n\right),$$

其中 $\varphi(n)$ 为 Euler 函数, $d(n)$ 为除数函数, $\omega(n)$ 表示 n 的所有不同素因子的个数

2 若干引理

引理1[1] 设 m、n、q 为整数, 则对模 q 的任一Dirichlet 函数 χ, 有估计式

* 1995年12月19日收到 1998年7月2日收到修改稿

$$\sum_{a=1}^{q}{}' \chi(a) e\left(\frac{ma+na^{-}}{q}\right) \ll (m,n,q)^{\frac{1}{4}} q^{\frac{1}{2}} d(q),$$

其中 (m,n,q) 表示 m、n、q 三个数的最大公因数，$\sum_{a=1}^{q}{}'$ 表示对与 q 互素的 a 求和，$e(a) = e^{2\pi i a}$.

引理2[2] 设模 $n \geq 3$ 存在原根，则有下面估计式

$$\sum_{\substack{a=1\\ ab\equiv 1(n)\\ a,b\in A}}^{n}\sum_{b=1}^{n} e\left(\frac{ra+sb}{n}\right) \ll (r,s,n)^{\frac{1}{4}} n^{\frac{1}{2}} 4^{\omega(\varphi(n))} d(n).$$

引理3 设整数 $q \geq 3$，对任意整数 n 和非负整数 r 及实数 $0 < x \leq 1$，定义 $K(x,n,r) = \sum_{a\leq xq} a^r e\left(\frac{an}{q}\right)$ 有估计式

$$K(x,n,r) \begin{cases} = \dfrac{(xq)^{r+1}}{r+1} + O(q^r), & q \mid n, \\ \ll \dfrac{q^r}{\left|\sin\dfrac{\pi n}{q}\right|}, & q \nmid n. \end{cases}$$

证明 若 $q \mid n$，则有

$$K(x,n,r)\left(1 - e\left(\frac{n}{q}\right)\right) = e\left(\frac{n}{q}\right) - [xq]^r e\left(\frac{([xq]+1)n}{q}\right) + \sum_{a=1}^{[xq]-1}((a+1)^r - a^r) e\left(\frac{n(a+1)}{q}\right) \ll q^r + \sum_{a=1}^{[xq]-1}((a+1)^r - a^r) \ll q^r,$$

于是有

$$K(x,n,r) \ll \frac{q^r}{\left|\sin\dfrac{\pi n}{q}\right|}.$$

若 $q \nmid n$，则有

$$K(x,n,r) = \sum_{a\leq xq} a^r = \int_0^{[xq]} t^r dt + O(q^r) = \frac{(xq)^{r+1}}{r+1} + O(q^r).$$

引理4 设模 $n \geq 3$ 存在原根，对任意非负整数 r, s 和实数 $0 < x, y \leq 1$，有估计式

$$\sum_{\substack{a\leq xn\\ b\leq yn\\ ab\equiv 1(n)\\ a,b\in A}}\sum a^r b^s = \frac{\varphi(\varphi(n)) n^{r+s} x^{r+1} y^{s+1}}{(r+1)(s+1)} + O(n^{r+s+\frac{1}{2}} d^2(n) 4^{\omega(\varphi(n))} \ln^2 n).$$

证明 注意到三角恒等式

$$\sum_{a=1}^{n} e\left(\frac{am}{n}\right) = \begin{cases} n, & n \mid m, \\ 0, & n \nmid m \end{cases} \tag{1}$$

及引理3，有

$$\sum_{\substack{a\leq xn\\ b\leq yn\\ ab\equiv 1(n)\\ a,b\in A}}\sum a^r b^s = \frac{1}{n^2}\sum_{u,v=1}^{n}\left(\sum_{\substack{a=1\\ ab\equiv 1(n)\\ a,b\in A}}^{n}\sum_{b=1}^{n} e\left(\frac{au+bv}{n}\right)\right)\left(\sum_{c=1}^{[xn]} c^r e\left(-\frac{cu}{n}\right)\right)\left(\sum_{d=1}^{[yn]} d^s e\left(-\frac{dv}{n}\right)\right)$$

$$= \frac{x^{r+1} y^{s+1} n^{r+s} \varphi(\varphi(n))}{(r+1)(s+1)} + O(n^{r+s+\frac{1}{2}} d^2(n) 4^{\omega(\varphi(n))} \ln^2 n).$$

引理5 设模 $n \geq 3$ 存在原根，对任意非负整数 k 和实数 $0 < x, y \leq 1$，有

$$\sum_{\substack{a\le xn\\ \bar a\le yn\\ a\in A}}(a-\bar a)^{2k}=\frac{\varphi(\varphi(n))n^{2k}}{(2k+1)(2k+2)}(x^{2k+2}+y^{2k+2}-(x-y)^{2k+2})+$$

$$O(4^k n^{2k+\frac12}d^2(n)4^{\omega(\varphi(n))}\ln^2 n).$$

证明 由二项式公式及引理4得

$$\sum_{\substack{a\le xn\\ \bar a\le yn\\ a\in A}}(a-\bar a)^{2k}=\sum_{i=0}^{2k}\binom{2k}{i}(-1)^i\sum_{\substack{a\le xn\\ \bar a\le yn\\ a\in A}}a^{2k-i}(\bar a)^i$$

$$=\frac{\varphi(\varphi(n))n^{2k}}{(2k+1)(2k+2)}\left(-\sum_{i=0}^{2k+2}(-1)^i\binom{2k+2}{i}x^{2k-i+2}y^i+x^{2k+2}+y^{2k+2}\right)+$$

$$O(4^k n^{2k+\frac12}d^2(n)4^{\omega(\varphi(n))}\ln^2 n)$$

$$=\frac{\varphi(\varphi(n))n^{2k}}{(2k+1)(2k+2)}\left(x^{2k+2}y^{2k+2}-(x-y)^{2k+2}\right)+O(4^k n^{2k+\frac12}d^2(n)4^{\omega(\varphi(n))}\ln^2 n)$$

引理6[3] 设 u,h 及 k 为整数, 且 $k\ge 1$, 则有有限 Fourier 展开式

$$\left(\left(\frac{uh}{k}\right)\right)=-\frac{1}{2k}\sum_{r=1}^{k-1}\sin\frac{2\pi rhu}{k}\operatorname{ctg}\frac{\pi r}{k},$$

其中函数 $((x))$ 定义为

$$((x))=\begin{cases}x-[x]-\dfrac12, & \text{如果 } x \text{ 不是整数},\\ 0, & \text{如果 } x \text{ 是整数}\end{cases}$$

引理7 设模 $n\ge 3$ 存在原根, 对任意非负整数 k 和实数 $0<x,y\le 1$, 有估计式

$$\sum_{\substack{a\le xn\\ \bar a\le yn\\ a\in A}}(a-\bar a)^{2k+1}\left(\left(\frac{a-\bar a}{n}\right)\right)\ll n^{2k+\frac32}d^2(n)4^{\omega(\varphi(n))}\ln^4 n.$$

证明 由引理2, 引理3, 引理6及三角恒等式(1)可得

Ⅰ) 当 $0<x\le\frac12, 0<y\le\frac12$ 时,

$$\sum_{\substack{a\le xn\\ \bar a\le yn\\ a\in A}}(a-\bar a)^{2k+1}\left(\left(\frac{a-\bar a}{n}\right)\right)$$

$$=-\frac{1}{2n^2}\sum_{r=1}^{n-1}\operatorname{ctg}\frac{\pi r}{n}\sum_{m=1}^{n}\left(\sum_{t=1}^{[xn]}\sum_{\substack{a=1\\ ab\equiv 1(n)\\ a,b\in A}}^{[xn]}\sum_{b=1}^{[yn]}t^{2k+1}\sin\frac{2\pi r(a-b)}{n}e\left(\frac{m(a-b-t)}{n}\right)+\right.$$

$$\left.\sum_{t=1}^{[yn]}\sum_{\substack{a=1\\ ab\equiv 1(n)\\ a,b\in A}}^{[xn]}\sum_{b=1}^{[yn]}t^{2k+1}\sin\frac{2\pi r(b-a)}{n}e\left(\frac{m(b-a-t)}{n}\right)\right)+O(n^{2k+1}d(n)\ln n). \qquad (2)$$

现估计(2)式中各项, 注意到三角恒等式 $\sin(2\pi rx)=\frac{1}{2i}\left(e(rx)-e(-rx)\right)$ 得

$$\sum_{\substack{a=1\\ab\equiv 1(n)\\ a,b\in A}}^{[xn]}\sum_{b=1}^{[yn]} e\left(\frac{m(a-b)}{n}\right) e\left(\frac{\pm r(a-b)}{n}\right)$$

$$= \frac{1}{n^2}\sum_{u=1}^{n}\sum_{v=1}^{n}\sum_{\substack{a=1\\ab\equiv 1(n)\\ a,b\in A}}^{n}\sum_{b=1}^{n} e\left(\frac{(u+m\pm r)a+(v-(m\pm r))b}{n}\right)\left(\sum_{c=1}^{[xn]} e\left(-\frac{uc}{n}\right)\right)\left(\sum_{d=1}^{[yn]} e\left(-\frac{dv}{n}\right)\right)$$

$$\ll n^{\frac{1}{2}}(m\pm r,n)^{\frac{1}{4}} d(n) 4^{\omega(\varphi(n))} + n^{\frac{1}{2}} d^2(n) 4^{\omega(\varphi(n))} \ln^2 n.$$

同理可得

$$\sum_{\substack{a=1\\ab\equiv 1(n)\\ a,b\in A}}^{[xn]}\sum_{b=1}^{[yn]} e\left(\frac{m(b-a)}{n}\right) e\left(\frac{\pm r(b-a)}{n}\right) \ll n^{\frac{1}{2}}((m\pm r,n)^{\frac{1}{4}} + d(n)\ln^2 n) d(n) 4^{\omega(\varphi(n))}.$$

于是

$$\sum_{\substack{a\le xn\\ \bar{a}\le yn\\ a\in A}} (a-\bar{a})^{2k+1}\left(\left(\frac{a-\bar{a}}{n}\right)^{+}\right) \ll \frac{1}{n^2}\sum_{r=1}^{n-1}\frac{n}{r} n^{2k+2} n^{\frac{1}{2}} d(n) 4^{\omega(\varphi(n))}((r,n)^{\frac{1}{4}} + d(n)\ln^2 n) +$$

$$\frac{1}{n^2}\sum_{r=1}^{n-1}\sum_{m=1}^{n-1}\frac{n}{r}\frac{n^{2k+2}}{m} n^{\frac{1}{2}} d(n) 4^{\omega(\varphi(n))}\left((m\pm r,n)^{\frac{1}{4}} + d(n)\ln^2 n\right) \ll n^{2k+\frac{3}{2}} d^2(n) 4^{\omega(\varphi(n))}\ln^4 n.$$

Ⅱ) **当** $\frac{1}{2} < x \le 1, \frac{1}{2} < y \le 1$ **时,**

$$\sum_{\substack{a\le xn\\ \bar{a}\le yn\\ a\in A}} (a-\bar{a})^{2k+1}\left(\left(\frac{a-\bar{a}}{n}\right)^{+}\right)$$

$$= -\frac{1}{2n}\sum_{r=1}^{n-1}\operatorname{ctg}\frac{\pi r}{n}\left(\sum_{\substack{a=1\\ab\equiv 1(n)\\ 0<a-b\le n/2\\ a,b\in A}}^{[xn]}\sum_{b=1}^{[yn]} (a-b)^{2k+1}\sin\frac{2\pi r(a-b)}{n} + \right.$$

$$\sum_{\substack{a=1\\ab\equiv 1(n)\\ a-b>n/2\\ a,b\in A}}^{[xn]}\sum_{b=1}^{[yn]} (a-b)^{2k+1}\sin\frac{2\pi r(a-b)}{n} + \sum_{\substack{a=1\\ab\equiv 1(n)\\ 0<b-a\le n/2\\ a,b\in A}}^{[xn]}\sum_{b=1}^{[yn]} (b-a)^{2k+1}\sin\frac{2\pi r(b-a)}{n} +$$

$$\left.\sum_{\substack{a=1\\ab\equiv 1(n)\\ b-a>n/2\\ a,b\in A}}^{[xn]}\sum_{b=1}^{[yn]} (b-a)^{2k+1}\sin\frac{2\pi r(b-a)}{n}\right) \ll n^{2k+\frac{3}{2}} d^2(n) 4^{\omega(\varphi(n))}\ln^4 n.$$

Ⅲ) **当** $0 < x \le \frac{1}{2}, \frac{1}{2} < y \le 1$ **时,**

$$\sum_{\substack{a\le xn\\ \bar{a}\le yn\\ a\in A}} (a-\bar{a})^{2k+1}\left(\left(\frac{a-\bar{a}}{n}\right)^{+}\right) \ll n^{2k+\frac{3}{2}} d^2(n) 4^{\omega(\varphi(n))}\ln^4 n.$$

结合Ⅰ)、Ⅱ)、Ⅲ), 于是完成了引理7的证明

3 定理的证明

有了上一节的几个引理, 容易给出定理的证明 事实上, 由引理5, 引理6, 引理7可得

$$\sum_{\substack{a\leq xn\\ \bar{a}\leq yn\\ a\in A}}\left|a-\bar{a}\right|^{2k+1}=\sum_{\substack{a\leq xn\\ \bar{a}\leq yn\\ a>\bar{a}\\ a\in A}}(a-\bar{a})^{2k+1}+\sum_{\substack{a\leq xn\\ \bar{a}\leq yn\\ \bar{a}>a\\ a\in A}}(\bar{a}-a)^{2k+1}$$

$$=\sum_{\substack{a\leq xn\\ \bar{a}\leq yn\\ a\in A}}\left(\frac{a-\bar{a}}{n}+\frac{1}{2}-\left(\left(\frac{a-\bar{a}}{n}\right)\right)\right)(a-\bar{a})^{2k+1}+$$

$$\sum_{\substack{a\leq xn\\ \bar{a}\leq yn\\ a\in A}}\left(\frac{\bar{a}-a}{n}+\frac{1}{2}-\left(\left(\frac{\bar{a}-a}{n}\right)\right)\right)(\bar{a}-a)^{2k+1}$$

$$=\frac{2}{n}\frac{\varphi(\varphi(n))n^{2k+2}}{(2k+3)(2k+4)}\left(x^{2k+4}+y^{2k+4}-(x-y)^{2k+4}\right)+$$

$$O\left(4^{k+1}n^{2k+\frac{3}{2}}d^2(n)4^{\omega(\varphi(n))}\ln^2 n\right)+O\left(n^{2k+\frac{3}{2}}d^2(n)4^{\omega(\varphi(n))}\ln^4 n\right)$$

$$=\frac{\varphi(\varphi(n))n^{2k+1}}{(2k+3)(k+2)}\left(x^{2k+4}+y^{2k+4}-(x-y)^{2k+4}\right)+$$

$$O\left(4^k n^{2k+\frac{3}{2}}d^2(n)4^{\omega(\varphi(n))}\ln^4 n\right).$$

于是完成了定理的证明

参 考 文 献

1 Weil A. *On some exponential sums*. Proc Nat Acad Sci, USA, 1948, **34**: 204-207

2 王辉, 胡志兴, 高丽 关于模N的原根的逆及其整除性 数学学报, 1997, **40**(3): 429-436

3 Apostol T M. *Modular Functions and Dirichlet Series in Number Theory*. Springer-Verlag, 1976

On the Odd Power of the Difference between the Primitive Root and Its Inverse Modulo N with Generalization

Wang Hui[1] *Wang Shiqin*[2] *Hu Zhixing*[3] *Gao Li*[1]

([1] Yan'an University, Yan'an 716000)

([2] Yan'an Agricultur School, Yan'an 716000)

([3] Beijing University of Aeronautics & Astronautics, 100083)

Abstract

We study the distribution properties of the difference between the primitive root a and its inverse $\bar{a}$ modulo n, and give an asymptotic formula for $\sum_{\substack{a\leq xn\\ \bar{a}\leq yn\\ a\in A}}\left|a-\bar{a}\right|^{2k+1}$.

Keywords primitive root, inverse, distribution property, asymptotic formula