1996年8月 第26卷第4期 西北大学学报(自然科学版) Journal of Northwest University(Natural Science Edition) Aug. 1996 Vol. 26 No. 4

关于模 q 的原根中 D. H. Lehmer 数与逆的差的分布*

王 辉[1] 高 丽[1] 胡志兴[2]

(1)西北大学数学系,710069,西安;2)延安大学数学系,716000,延安;第一作者30岁,女,硕士生)

摘 要 设奇数 $q\geqslant 3$ 存在原根,研究模 q 的原根中 D. H. Lehmer 数与它的逆的差的分布性质,并给出了一个较强的渐近公式。

关键词 原根;勒默数;逆;分布性质;渐近公式

分类号 O156.4

设 $q\geqslant 3$ 是奇数,对任一整数 $1\leqslant a\leqslant q-1$ 且 $(a,q)=1$,显然存在唯一的整数 $1\leqslant \bar{a}\leqslant q-1$,使得 $a\bar{a}\equiv 1(\mathrm{mod}\ q)$,如果 a 与 $\bar{a}$ 具有相反的奇偶性,则我们把这样的数 a 称为D. H. Lehmer 数。文献[1]研究了模 q 的D. H. Lehmer数和它的逆的分布性质,并证明了对任意奇数 q 有渐近公式

$$M(q,k)=\sideset{}{'}\sum_{\substack{a=1\\ 2\mid a+\bar{a}-1}}^{q}(a-\bar{a})^{2k}=\frac{\varphi(q)q^{2k}}{(2k+1)(2k+2)}+O(4^k q^{2k+\frac{1}{2}}d^2(q)\ln^2 q)。$$

若 $q\geqslant 3$ 存在原根,则对模 q 的任一原根 $1\leqslant a\leqslant q-1$,显然 $1\leqslant\bar{a}\leqslant q-1$ 也是模 q 的原根。设 A 表示区间[1,q]中模 q 的所有原根之集合,本文利用广义Kloostermann和估计及三角和方法来研究模 q 的原根中 D. H. Lehmer 数与它的逆的差的分布性质,设实数 $0<x,y\leqslant 1$,定义

$$M_0(q,R)=\sum_{\substack{a\leqslant xq\\ \bar{a}\leqslant yq\\ a\in A\\ 2\mid a+\bar{a}-1}}(a-\bar{a})^{2k} \tag{1}$$

证明了下面的结论。

定理 设奇数 $q\geqslant 3$ 存在原根,对任意非负整数 k,对任意实数 $0<x,y\leqslant 1$,有 $M_0(q,k)=\frac{\varphi(\varphi(q))q^{2k}}{4(k+1)(2k+1)}(x^{2k+2}+y^{2k+2}-(x-y)^{2k+2})+O(4^k q^{2k+\frac{3}{4}4^{\omega(\varphi(q))}d^2(q)\ln^2 q)$ 其中 $\varphi(q)$ 为Euler函数,$\omega(n)$ 表示 n 的所有不同素因子的个数,$d(q)$ 为除数函数。

1 基本引理

为了完成定理的证明,需要用几个辅助引理。

引理1 设模 $n\geqslant 3$ 存在原根,则对任意正整数 $(m,n)=1$,有下面的

$$\sum_{k\mid\varphi(n)}\frac{\mu(k)}{\varphi(k)}\sideset{}{^*}\sum_{a=1}^{k}e\left(\frac{a\ \mathrm{ind}m}{k}\right)=\begin{cases}\dfrac{\varphi(n)}{\varphi(\varphi(n))}, & m\text{ 为 }n\text{ 的原根};\\ 0, & \text{其他}。\end{cases}$$

其中 $\mu(n)$ 为 Mobius 函数,ind$m$ 表示 m 相对模 n 的某一给定原根的指标,$e(y)=e^{2\pi iy}$,$\sideset{}{^*}\sum_{a=1}^{k}$ 表示对与 k

* 陕西省教委专项基金资助课题

收稿日期:1995-06-29

互素的 a 求和。

证明 参阅文献 2 或 3。

引理 2 设模 $q \geqslant 3$ 存在原根，则有下面的估计式

$$\sum_{\substack{a=1\\ ab\equiv 1(q)\\ a,b\in A}}^{q}\sum_{b=1}^{q} e\left(\frac{ra+sb}{q}\right) << (r,s,q)^{\frac{1}{4}} q^{\frac{3}{4}} 4^{\omega(\varphi(q))} d(q)。$$

证明 参阅文献4。

引理 3 设 q 是奇数，对任意整数 n 和非负整数 r，实数 $0 < x \leqslant 1$，定义 $K(x,n,r) = \sum_{a\leqslant xq} a^r e\left(\frac{an}{q}\right)$

$$H(x,n,r) = \sum_{a\leqslant xq} (-1)^a a^r e\left(\frac{an}{q}\right),$$

估计式为

$$K(x,n,r)\begin{cases} = \dfrac{(xq)^{r+1}}{r+1} + O(q^r), q \mid n; \\ << \dfrac{q^r}{\left|\sin\dfrac{\pi n}{q}\right|}, q \nmid n。 \end{cases} \tag{2}$$

$$H(x,n,r) << \frac{q^r}{\left|\cos\dfrac{\pi n}{q}\right|}。 \tag{3}$$

证明 首先证明(2)式。当 $r=0$ 时，若 $q \mid n$，由于 $e\left(\frac{an}{q}\right) = 1$，则有 $\sum_{a\leqslant xq} e\left(\frac{an}{q}\right) = [xq] = xq + O(1)$ 其中 $[z]$ 表示不超过实数 z 的最大整数。

若 $q \nmid n$，则有 $\sum_{a\leqslant xq} e\left(\frac{an}{q}\right) << \frac{1}{\left|1-e\left(\frac{n}{q}\right)\right|} << \frac{1}{\left|\sin\frac{\pi n}{q}\right|}$ 所以，当 $r=0$ 时，(2)式成立。

当 $r > 0$ 时，若 $q \nmid n$，则有 $K(x,n,r)\left(1-e\left(\frac{n}{q}\right)\right) = \left(1-e\left(\frac{n}{q}\right)\right)$。

$$\sum_{a\leqslant xq} a^r e\left(\frac{an}{q}\right) = e\left(\frac{n}{q}\right) - [xq]^r e\left(\frac{([xq]+1)n}{q}\right) + \sum_{a=1}^{[xq]-1} ((a+1)^r - a^r) e\left(\frac{(a+1)n}{q}\right)$$

$$<< q^r + \sum_{a=1}^{[xq]-1} ((a+1)^r - a^r) << q^r,$$

于是有

$$K(x,n,r) << \frac{q^r}{\left|\sin\dfrac{\pi n}{q}\right|}。 \tag{4}$$

若 $q \mid n$，则有 $K(x,n,r) = \sum_{a\leqslant xq} a^r e\left(\frac{an}{q}\right) = \sum_{a=1}^{[xq]} a^r = \int_0^{[xq]} t^r \mathrm{d}t + O(q^r) = \frac{(xq)^{r+1}}{r+1} + O(q^r)$， (5)

结合(4)式及(5)式，得到(2)式。

现证明(3)式 $H(x,n,r)\left(1+e\left(\frac{n}{q}\right)\right) = \left(1+e\left(\frac{n}{q}\right)\right)$。

$$\sum_{a\leqslant xq} (-1)^a a^r e\left(\frac{an}{q}\right) = -e\left(\frac{an}{q}\right) + (-1)^{[xq]}[xq]^r e\left(\frac{([xq]+1)n}{q}\right)$$

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

$$<< (xq)^r + \sum_{a=1}^{[xq]-1} ((a+1)^r - a^r) << q^r。 \tag{6}$$

注意到 $\left|1+e\left(\frac{n}{q}\right)\right| = 2\left|\cos\frac{\pi n}{q}\right|$，由(6)式就得到(3)式。于是完成了引理 3 的证明。

引理 4 设 r，s 为非负整数，$q \geqslant 3$ 为奇数，有估计式

$$\sum_{\substack{a\leqslant xq\\ ab\equiv 1(q)\\ a,b\in A}}\sum_{b\leqslant yq} a^r b^s = \frac{\varphi(\varphi(q))q^{r+s}x^{r+1}y^{s+1}}{(r+1)(s+1)} + O(q^{r+s}+q^{\frac{3}{4}}4^{\omega(\varphi(q))}d^2(q)\ln^2 q)。$$

证明　注意到三角恒等式 $\sum_{a=1}^{q} e(\frac{an}{q}) = \begin{cases} q, & q \mid n; \\ 0, & q \nmid n。 \end{cases}$ (7)

有
$$\sum_{\substack{a\leqslant q\\ ab\equiv 1(q)\\ a,b\in A}}\sum_{\substack{b\leqslant q\\ a,b\in A}} a^r b^s = \frac{1}{q^2}\sum_{m,n=1}^{q}\Big(\sum_{\substack{a=1\\ ab\equiv 1(q)\\ a,b\in A}}^{q}\sum_{b=1}^{q} e\Big(\frac{am+bn}{q}\Big)\Big)\Big(\sum_{c=1}^{[sq]} c^s e\Big(-\frac{cm}{q}\Big)\sum_{d=1}^{[rq]} d^r e\Big(-\frac{nd}{q}\Big)\Big)$$
$$= \frac{1}{q^2}\sum_{m,n=1}^{q}\Big(\sum_{\substack{a=1\\ ab\equiv 1(q)\\ a,b\in A}}^{q}\sum_{b=1}^{q} e\Big(\frac{am+bn}{q}\Big)\Big)K(x,-m,r)K(y,-n,s)$$
$$= \frac{1}{q^2}\Big(\sum_{\substack{a=1\\ ab\equiv 1(q)\\ a,b\in A}}^{q}\sum_{b=1}^{q} 1\Big)K(x,-q,r)K(y,-q,s) + \frac{1}{q^2}\sum_{m=1}^{q-1}\Big(\sum_{\substack{a=1\\ ab\equiv 1(q)\\ a,b\in A}}^{q}\sum_{b=1}^{q} e\Big(\frac{am+bq}{q}\Big)\Big)$$
$$K(x,-m,r)K(y,-q,s) + \frac{1}{q^2}\sum_{n=1}^{q-1}\sum_{\substack{a=1\\ ab\equiv 1(q)\\ a,b\in A}}^{q}\sum_{b=1}^{q} e\Big(\frac{aq+bn}{q}\Big)K(x,-q,r)K(y,-n,s)$$
$$+ \frac{1}{q^2}\sum_{m=1}^{q-1}\sum_{n=1}^{q-1}\Big(\sum_{\substack{a=1\\ ab\equiv 1(q)\\ a,b\in A}}^{q}\sum_{b=1}^{q} e\Big(\frac{am+bn}{q}\Big)\Big)K(x,-m,r)K(y,-n,s)。 \quad (18)$$

其中 $K(x,-m,r)$ 是引理3中所定义的。由(2)式以及引理2，并注意到 $|\sin\frac{\pi m}{q}| >> \frac{m}{q}(1\leqslant m\leqslant q-1)$，有 $\frac{1}{q^2}\Big(\sum_{\substack{a=1\\ ab\equiv 1(q)\\ a,b\in A}}^{q}\sum_{b=1}^{q} 1\Big)K(x,-q,r)K(y,-q,s) = \frac{\varphi(\varphi(q))q^{r+s}x^{r+1}y^{s+1}}{(r+1)(s+1)} + O(q^{r+s})$ (9)

$$\frac{1}{q^2}\sum_{n=1}^{q-1}\Big(\sum_{\substack{a=1\\ ab\equiv 1(q)\\ a,b\in A}}^{q}\sum_{b=1}^{q} e\Big(\frac{aq+bn}{q}\Big)\Big)K(x,-q,r)K(y,-n,s)$$
$$<< q^{r+s+\frac{3}{4}}4^{\omega(\varphi(q))}d(q)\sum_{n=1}^{q-1}\frac{(q,n)^{\frac{1}{4}}}{qn} << q^{r+s+\frac{3}{4}}4^{\omega(\varphi(q))}d^2(q)\ln q, \quad (10)$$

同理可得
$$\frac{1}{q^2}\sum_{m=1}^{q-1}\Big(\sum_{\substack{a=1\\ ab\equiv 1(q)\\ a,b\in A}}^{q}\sum_{b=1}^{q} e\Big(\frac{am+bq}{q}\Big)\Big)K(x,-m,r)K(y,-q,s)$$
$$<< q^{r+s+\frac{3}{4}}4^{\omega}(\varphi(q))d^2(q)\ln q \quad (11)$$
$$\frac{1}{q^2}\sum_{m=1}^{q-1}\sum_{n=1}^{q-1}\Big(\sum_{\substack{a=1\\ ab\equiv 1(q)\\ a,b\in A}}^{q}\sum_{b=1}^{q} e\Big(\frac{am+bn}{q}\Big)\Big)K(x,-m,r)K(y,-n,s)$$
$$<< q^{r+s+\frac{3}{4}}4^{\omega(\varphi(q))}d(q)\sum_{m=1}^{q-1}\sum_{n=1}^{q-1}\frac{(m,n,q)^{\frac{1}{4}}}{mn} << q^{r+s+\frac{3}{4}}4^{\omega(\varphi(q))}d(q)\ln^2 q。 \quad (12)$$

把(9)～(12)代入(8)得
$$\sum_{\substack{a\leqslant q\\ ab\equiv 1(q)\\ a,b\in A}}\sum_{\substack{b\leqslant q\\ a,b\in A}} a^r b^s = \frac{\varphi(\varphi(q))q^{r+s}x^{r+1}y^{s+1}}{(r+1)(s+1)} + O(q^{r+s+\frac{3}{4}}4^{\omega(\varphi(q))}d^2(q)\ln^2 q),$$

于是完成引理4的证明。

引理5　设 r,s 为非负整数，$q\geqslant 3$ 为奇数，则有
$$\sum_{\substack{a\leqslant q\\ ab\equiv 1(q)\\ a,b\in A}}\sum_{\substack{b\leqslant q\\ a,b\in A}} (-1)^{a+b}a^r b^s = O(q^{r+s+\frac{3}{4}}4^{\omega(\varphi(q))}d^2(q)\ln^2 q)。$$

证明　类似地，得到
$$\sum_{\substack{a\leqslant q\\ ab\equiv 1(q)\\ a,b\in A}}\sum_{\substack{b\leqslant q\\ a,b\in A}} (-1)^{a+b}a^r b^s = \frac{1}{q^2}\sum_{\substack{a=1\\ ab\equiv 1(q)\\ a,b\in A}}^{q}\sum_{b=1}^{q}\sum_{c\leqslant q}(-1)^c c^r\sum_{d\leqslant q}(-1)^d d^s\sum_{m=1}^{q}\sum_{n=1}^{q} e\Big(\frac{m(a-c)+n(b-d)}{q}\Big)$$

$$= \frac{1}{q^2}\sum_{m=1}^{q}\sum_{n=1}^{q}\Big(\sum_{\substack{a=1\\ ab\equiv 1(q)\\ a,b\in A}}^{q}\sum_{b=1}^{q} e\Big(\frac{ma+nb}{q}\Big)\Big)H(x,-m,r)H(y,-n,s), \tag{13}$$

这里 $H(x,-m,r)$ 是引理 3 中所定义的。注意到 $|\cos\frac{\pi m}{q}| = |\sin\frac{\pi(q-2m)}{2q}|$ 及 $q-2m\neq 0$。由(3)式和使用引理 4 中的证明方法，容易推出引理 5 的结论。

2　定理的证明

由二项式公式、引理 4、引理 5 得

$$\begin{aligned}
M_0(q,k) &= \sum_{\substack{0\leqslant a\leqslant q\\ 0\leqslant \bar{a}\leqslant q\\ a\in A\\ 2\mid a+\bar{a}+1}} (a-\bar{a})^{2k} = \frac{1}{2}\sum_{\substack{0\leqslant a\leqslant q\\ ab\equiv 1(q)\\ a,b\in A}}\sum_{b\leqslant q}(1-(-1)^{a+b})(a-b)^{2k}\\
&= \frac{1}{2}\sum_{i=0}^{2k}\binom{2k}{i}(-1)^i\Big(\sum_{\substack{a\leqslant q\\ \bar{a}\leqslant q\\ a\in A}} a^{2k-i}(\bar{a})^i - \sum_{\substack{a\leqslant q\\ \bar{a}\leqslant q\\ a\in A}}(-1)^{a-\bar{a}}a^{2k-i}(\bar{a})^i\Big)\\
&= \frac{1}{2}\sum_{i=0}^{2k}\binom{2k}{i}(-1)^i\Big(\frac{\varphi(\varphi(q))q^{2k}x^{2k-i+1}y^{i+1}}{(i+1)(2k-i+1)} + O(q^{2k+\frac{3}{4}}4^{\omega(\varphi(q))}d^2(q)\ln^2 q)\Big)\\
&+ O\Big(\sum_{i=0}^{2k}\binom{2k}{i}q^{2k+\frac{3}{4}}4^{\omega(\varphi(q))}d^2(q)\ln^2 q\Big)\\
&= \frac{\varphi(\varphi(q))q^{2k}}{4(k+1)(2k+1)}\sum_{i=0}^{2k}(-1)^i\binom{2k+2}{i+1}x^{2k-i+1}y^{i+1} + O(4^k q^{2k+\frac{3}{4}}4^{\omega(\varphi(q))}d^2(q)\ln^2 q)\\
&= \frac{\varphi(\varphi(q))q^{2k}}{4(k+1)(2k+1)}\Big(-\sum_{i=0}^{2k+2}(-1)^i\binom{2k+2}{i}x^{2k-i+2}y^i + x^{2k+2}+y^{2k+2}\Big)\\
&+ O(4^k q^{2k+\frac{3}{4}}4^{\omega(\varphi(q))}d^2(q)\ln^2 q)\\
&= \frac{\varphi(\varphi(q))q^{2k}}{4(k+1)(2k+1)}(x^{2k+2}+y^{2k+2}-(x-y)^{2k+2}) + O(4^k q^{2k+\frac{3}{4}}4^{\omega(\varphi(q))}d^2(q)\ln^2 q),
\end{aligned}$$

于是完成定理的证明。

对张文鹏教授的精心指导表示衷心的感谢！

参 考 文 献

1　Zhang Wengpeng. On the difference between a D. H. Lehmer number and its inverse modulo q, Acta Arithmetica, LXV Ⅲ. 1994(3):255～263

2　王巨平. 关于 Golomb 猜想. 中国科学(A 辑),1987(9):927～935

3　潘承洞,潘承彪. 哥德巴赫猜想. 北京:科学出版社,1981

4　王辉,胡志兴,高丽. 关于模 N 的原根及其整除性的推广. 延安大学学报(自然科学版),1995,14(3):12～16

责任编辑　张素敏

On the Difference of D. H. Lehmer Number and Its Inverse in the Primitive Roots Modulo q

Wang Hui[1)]　Gao Li[1)]　Hu Zhixing[2)]

(1)Department of Mathematics, Northwest University, 710069, Xi'an;

2)Department of Mathematics, Yan'an University, 716000, Yan'an)

Abstract　Let $q\geqslant 3$ be odd integer, and modulo q contains a primitive root. It is to study the distribution properties on the difference of D. H. Lehmer number and its inverse in the primitive roots modulo q, and give a sharper asymptotic formula.

Key words　primitive root; D. H. Lehmer number; inverse; distribution property; asymptotic formula