1998年4月 第28卷第2期 西北大学学报(自然科学版) Journal of Northwest University(Natural Science Edition) Apr. 1998 Vol. 28 No. 2

③ 105-108

二次剩余原根及其Gallapher型问题†

武胜利

(西北大学数学系,710069,西安;28岁,硕士)

0156.4

摘 要 利用三角和转换与某种特征和的估计,给出了涉及二次剩余及原根的两个伽利佛问题的渐近公式。

关键词 二次剩余;原根;均值;渐近公式;伽利佛问题

分类号 O156.4

张文鹏教授在访问美国乔治亚大学期间解决了P. Gallapher教授所提出的一个如下形式的均值问题

$$S(p,u)=\sum_{x=1}^{p}\Big|\frac{1}{2}\sum_{x<a\leqslant x+u}^{'}1-\frac{1}{2}\sum_{x<a\leqslant x+u}^{'}1\Big|^2, \tag{1}$$

其中$\sum_{a}^{'}$表示对与素数p互素的a求和,而$a\bar{a}\equiv 1(\mathrm{mod}\,p)$且$1\leqslant\bar{a}\leqslant p-1$。

张文鹏教授研究了$S(p,u)$的渐近性质[1],并得出

$$S(p,u)=\frac{up}{4}+O(u^2\sqrt{p}\ln^2 p),u<\sqrt{p}。$$

其中大O常数为绝对常数。

这一工作事实上是张文鹏教授关于D. H. Lehmer问题研究的延伸。我们称具有式(1)形式的均值问题为P. Gallapher型,并就二次剩余及原根的情形得到了如下结果:

定理1 设p是素数,u为整数且$0<u<p$,则有

$$S(p,u)=\sum_{x=1}^{p}|E(p,u,x)|^2=\frac{up}{4}+O(u^2),\ u<p。$$

其中$E(p,u,x)=\frac{1}{2}\sum_{x<a\leqslant x+u}^{'}(1+(\frac{a}{p}))-\frac{1}{2}\sum_{x<a\leqslant x+u}^{'}1$,$\sum_{a}^{'}$表对与$p$互素的$a$求和,$(\frac{a}{p})$是legendre符号。

定理2 设p是一素数,u为整数且$0<u<\sqrt{p}$,则有

$$S(p,u)=\sum_{x=1}^{p}|E(p,u,x)|^2=u\varphi(p-1)-\frac{u\varphi^2(p-1)}{p-1}+O(u^2\sqrt{p}\,4^{\omega(p-1)}),u<\sqrt{p}。$$

其中,$E(p,u,x)=\sum_{x<a\leqslant x+u}^{'}1-\frac{\varphi(p-1)}{p-1}\sum_{x<a\leqslant x+u}^{'}1$,$\sum_{a}^{*}$表对模$p$的所有原根求和,$\sum_{a}^{'}$表对与$p$互素的$a$求和,$\varphi(n)$为Euler函数,$\omega(n)$表$n$的不同素因子的个数。

1 引 理

引理1 设p为一素数,t为一整数且$(p,t)=1$,则有

$$\sum_{\substack{a=1\\ a-b\equiv t(\mathrm{mod}\,p)}}^{p-1}\sum_{b=1}^{p-1}(\frac{ab}{p})=O(1)。$$

† 收稿日期:1997-06-16

1)Zhang Wenpeng. On a problem of P. Gallapher. Acta. Math. Hungar. (to appear)

证 由二次剩余的有关性质得

$$\sum_{\substack{a=1\\ a-b\equiv t(\mathrm{mod}\,p)}}^{p-1}\sum_{b=1}^{p-1}\left(\frac{ab}{p}\right)=\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\left(\frac{a+t}{p}\right)+O(1)$$

$$=\sum_{a=1}^{p-1}\left(\frac{1+t\bar{a}}{p}\right)+O(1)=\sum_{a=1}^{p-1}\left(\frac{a+1}{p}\right)+O(1)=O(1)。$$

证毕。

引理 2 设 n 为存在原根的整数,则有

$$\sum_{k\mid\varphi(n)}\frac{\mu(k)}{\varphi(k)}\sideset{}{'}\sum_{m=1}^{k}\mathrm{e}\left(\frac{m\mathrm{ind}a}{k}\right)=\begin{cases}\dfrac{\varphi(n)}{\varphi(\varphi(n))},\text{如 } a \text{ 为模 } n \text{ 的原根;}\\ 0,\qquad\quad \text{否则。}\end{cases}$$

其中 $\sum\limits_{m}'$ 表对与 k 互素的 m 求和,$\mathrm{e}(y)=\mathrm{e}^{2\pi iy}$,$\mu(n)$ 表 Möbius 函数,$\mathrm{ind}a$ 表 a 相对于模 n 某一固定原根的指标。

证 参阅文献[1]。

引理 3 设 χ_1,χ_2 为模 p 的非主特征,则有

$$\sum_{\substack{a=1\\ a-b\equiv t(\mathrm{mod}\,p)}}^{p-1}\sum_{b=1}^{p-1}\chi_1(a)\chi_2(b)=O(\sqrt{p})。$$

证 由三角和恒等式

$$\sum_{a=1}^{m}\mathrm{e}\left(\frac{an}{m}\right)=\begin{cases}m,\text{如 } m\mid n;\\ 0,\quad \text{否则。}\end{cases}\tag{2}$$

可知

$$\sum_{\substack{a=1\\ a-b\equiv t(\mathrm{mod}\,p)}}^{p-1}\sum_{b=1}^{p-1}\chi_1(a)\chi_2(b)=\sum_{a=1}^{p-1}\chi_1(a)\chi_2(a+t)+O(1)$$

$$=\frac{1}{p^2}\sum_{a=1}^{p}\sum_{c=1}^{p-1}\sum_{d=1}^{p-1}\chi_1(c)\chi_2(d)\sum_{r=1}^{p}\mathrm{e}\left(\frac{a-c}{p}r\right)\sum_{s=1}^{p}\mathrm{e}\left(\frac{a+t-d}{p}s\right)+O(1)$$

$$=\frac{1}{p^2}\sum_{r=1}^{p}\sum_{s=1}^{p}\mathrm{e}\left(\frac{ts}{p}\right)\sum_{a=1}^{p}\mathrm{e}\left(\frac{r+s}{p}a\right)\sum_{c=1}^{p-1}\chi_1(c)\mathrm{e}\left(\frac{-rc}{p}\right)\sum_{d=1}^{p-1}\chi_2(d)\mathrm{e}\left(\frac{-sd}{p}\right)+O(1)$$

$$=\frac{1}{p^2}\sum_{r=1}^{p}\sum_{s=1}^{p}\mathrm{e}\left(\frac{ts}{p}\right)\bar{\chi}_1(-r)\bar{\chi}_2(-s)\sum_{c=1}^{p-1}\chi_1(c)\mathrm{e}\left(\frac{c}{p}\right)\sum_{d=1}^{p-1}\chi_2(d)\mathrm{e}\left(\frac{d}{p}\right)+O(1)。\tag{3}$$

由于 χ_1,χ_2 均为模 p 的非主特征,利用熟知的高斯和估计,再结合(2)和(3)就得到

$$\sum_{\substack{a=1\\ a-b\equiv t(\mathrm{mod}\,p)}}^{p-1}\sum_{b=1}^{p-1}\chi_1(a)\chi_2(b)=\frac{1}{p^2}G(1,\chi_1)G(1,\chi_2)\sum_{r=1}^{p-1}\bar{\chi}_1(-r)\bar{\chi}_2(r)\mathrm{e}\left(\frac{-tr}{p}\right)+O(1)$$

$$<<\left|\sum_{r=1}^{p-1}\bar{\chi}_1\bar{\chi}_2(r)\mathrm{e}\left(\frac{-tr}{p}\right)\right|+O(1)=O(\sqrt{p})。$$

这就证明了引理 3。

2 定理证明

证明定理 1

证 由三角和恒等式(2),我们得到

$$E(p,u,x)=\frac{1}{2}\sum_{x<a\leqslant x+u}'\left(1+\left(\frac{a}{p}\right)\right)-\frac{1}{2}\sum_{x<a\leqslant x+u}'1$$

$$=\frac{1}{2}\sum_{x<a\leqslant x+u}'\left(\frac{a}{p}\right)=\frac{1}{2p}\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\sum_{x<c\leqslant x+u}\sum_{r=1}^{p}\mathrm{e}\left(\frac{c-a}{p}r\right)$$

$$=\frac{1}{2p}\sum_{r=1}^{p}\sum_{a=1}^{p-1}\left(\frac{a}{p}\right)\mathrm{e}\left(\frac{-ar}{p}\right)\sum_{1\leqslant c\leqslant u}\mathrm{e}\left(\frac{rc+rx}{p}\right)。$$

从而，利用式(2)及引理 1 便有

$$S(p,u)=\sum_{x=1}^{p}|E(p,u,x)|^2$$

$$=\frac{1}{4p^2}\sum_{r=1}^{p}\sum_{s=1}^{p}\sum_{a=1}^{p-1}(\frac{a}{p})e(\frac{-ar}{p})\sum_{b=1}^{p-1}(\frac{b}{p})e(\frac{bs}{p})\sum_{c=1}^{u}\sum_{d=1}^{u}e(\frac{rc-sd}{p})\sum_{x=1}^{p}e(\frac{r-s}{p}x)$$

$$=\frac{1}{4p}\sum_{r=1}^{p}\sum_{a=1}^{p-1}(\frac{a}{p})e(\frac{-ar}{p})\sum_{b=1}^{p-1}(\frac{b}{p})e(\frac{br}{p})\sum_{1\leqslant c\leqslant u}\sum_{1\leqslant d\leqslant u}e(\frac{c-d}{p}r)$$

$$=\frac{1}{4}\sum_{a=1}^{p-1}\sum_{b=1}^{p-1}(\frac{ab}{p})\sum_{\substack{1\leqslant c\leqslant u\\ a-b\equiv c-d(\mathrm{mod}\,p)}}\sum_{1\leqslant d\leqslant u}1=\frac{u(p-1)}{4}+\frac{1}{4}\sum_{\substack{c,d=1\\ c\neq d}}^{u}\sum_{\substack{a,b=1\\ a-b\equiv c-d(\mathrm{mod}\,p)}}^{p-1}(\frac{ab}{p})$$

$$=\frac{u(p-1)}{4}+\frac{1}{2}\sum_{t=1}^{u-1}(u-t)\sum_{\substack{a=1\\ a-b\equiv r(\mathrm{mod}\,p)}}^{p-1}\sum_{b=1}^{p-1}=\frac{up}{4}+O(u^2),u<p。$$

这样便完成了定理 1 的证明。

证明定理 2。

证　由三角和恒等式(2)及引理 2 得

$$E(p,u,x)=\sum_{x<a\leqslant x+u}^{*}1-\frac{\varphi(p-1)}{p-1}\sum_{x<a\leqslant x+u}^{'}1$$

$$=\frac{\varphi(p-1)}{p-1}\sum_{k|p-1}\frac{\mu(k)}{\varphi(k)}\sum_{m=1}^{k}{}^{'}\sum_{x<a\leqslant x+u}^{'}e(\frac{m\mathrm{ind}a}{k})-\frac{\varphi(p-1)}{p-1}\sum_{x<a\leqslant x+u}^{'}1$$

$$=\frac{\varphi(p-1)}{p-1}\sum_{\substack{k|p-1\\ k>1}}\frac{\mu(k)}{\varphi(k)}\sum_{m=1}^{k}{}^{'}\sum_{x<a\leqslant x+u}^{'}e(\frac{m\mathrm{ind}a}{k})$$

$$=\frac{\varphi(p-1)}{p(p-1)}\sum_{\substack{k|p-1\\ k>1}}\frac{\mu(k)}{\varphi(k)}\sum_{m=1}^{k}{}^{'}\sum_{a=1}^{p-1}e(\frac{m\mathrm{ind}a}{k})\sum_{x<a\leqslant x+u}\sum_{r=1}^{p}e(\frac{a-c}{p}r)$$

$$=\frac{\varphi(p-1)}{p(p-1)}\sum_{r=1}^{p}\sum_{\substack{k|p-1\\ k>1}}\frac{\mu(k)}{\varphi(k)}\sum_{m=1}^{k}{}^{'}\sum_{a=1}^{p-1}e(\frac{m\mathrm{ind}a}{k})e(\frac{ar}{p})\sum_{1\leqslant c\leqslant u}e(\frac{-rc-rx}{p})。$$

这里，$\sum_{m}^{k}{}^{'}$ 表示对与 k 互素的 m 求和。进而，利用三角和转换得

$$S(p,u)=\sum_{x=1}^{p}|E(p,u,x)|^2=\frac{\varphi^2(p-1)}{p^2(p-1)^2}\sum_{r=1}^{p}\sum_{\substack{k|p-1\\ k>1}}\frac{\mu(k)}{\varphi(k)}\sum_{m=1}^{k}{}^{'}\sum_{a=1}^{p-1}e(\frac{ar}{p})$$

$$\sum_{c=1}^{u}e(\frac{-rc}{p})\sum_{s=1}^{p}\sum_{\substack{h|p-1\\ h>1}}\frac{\mu(h)}{\varphi(h)}\sum_{n=1}^{h}{}^{'}\sum_{b=1}^{p-1}e(\frac{-n\mathrm{ind}b}{h})e(\frac{-bs}{p})\sum_{d=1}^{u}e(\frac{sd}{p})\sum_{x=1}^{p}e(\frac{s-r}{p}x)$$

$$=\frac{\varphi^2(p-1)}{p(p-1)^2}\sum_{\substack{k|p-1\\ k>1}}\sum_{\substack{h|p-1\\ h>1}}\frac{\mu(k)\mu(h)}{\varphi(k)\varphi(h)}\sum_{m=1}^{k}{}^{'}\sum_{n=1}^{h}{}^{'}\sum_{\substack{a=1\\ a-b\equiv c-d(\mathrm{mod}\,p)}}^{p-1}\sum_{b=1}^{p-1}e(\frac{m\mathrm{ind}a}{k}-\frac{n\mathrm{ind}b}{h})\sum_{c=1}^{u}\sum_{d=1}^{u}1$$

$$=\frac{\varphi^2(p-1)}{(p-1)^2}\sum_{\substack{k|p-1\\ k>1}}\sum_{\substack{h|p-1\\ h>1}}\frac{\mu(k)\mu(h)}{\varphi(k)\varphi(h)}\sum_{m=1}^{k}{}^{'}\sum_{n=1}^{h}{}^{'}\sum_{a=1}^{p-1}e((\frac{m}{k}-\frac{n}{h})\mathrm{ind}a)\cdot u+$$

$$\frac{\varphi^2(p-1)}{(p-1)^2}\sum_{\substack{k|p-1\\ k>1}}\sum_{\substack{h|p-1\\ h>1}}\frac{\mu(k)\mu(h)}{\varphi(k)\varphi(h)}\sum_{m=1}^{k}{}^{'}\sum_{n=1}^{h}{}^{'}\sum_{\substack{a=1\\ a-b\equiv c-d(\mathrm{mod}\,p)\\ c\neq d}}^{p-1}\sum_{b=1}^{p-1}e(\frac{m\mathrm{ind}a}{k}-\frac{n\mathrm{ind}b}{h})\sum_{c,d=1}^{u}1。\qquad(4)$$

由 $(m,k)=(n,h)=1,k>1,h>1$ 可以知道 $e(\frac{m\mathrm{ind}a}{k})$ 和 $e(\frac{-n\mathrm{ind}b}{h})$ 均为模 p 的本原特征，且

$$\sum_{a=1}^{p-1}e((\frac{m}{k}-\frac{n}{h})\mathrm{ind}a)=\begin{cases}p-1,\text{如 } k=h \text{ 且 } m=n;\\ 0 \qquad\text{否则。}\end{cases}$$

再结合式(4)和引理 3，得

$$S(p,u)=\frac{u\varphi^2(p-1)}{p-1}\sum_{\substack{k|p-1\\ k>1}}\frac{\mu^2(k)}{\varphi(k)}+\frac{2\varphi^2(p-1)}{(p-1)^2}\sum_{\substack{k|p-1\\ k>1}}\sum_{\substack{h|p-1\\ h>1}}\sum_{t=1}^{u-1}(u-t)$$

$$\sum_{\substack{a=1\\a-b\equiv r(\mathrm{mod}\,p)}}^{p-1}\sum_{b=1}^{p-1} e\left(\frac{m\mathrm{ind}a}{k}\right)e\left(\frac{-n\mathrm{ind}b}{h}\right)=\frac{u\varphi^2(p-1)}{p-1}\sum_{\substack{k|p-1\\k>1}}\frac{\mu^2(k)}{\varphi(k)}+O(u^2\sqrt{p}\,4^{\omega(p-1)})$$

$$=u\varphi(p-1)-\frac{u\varphi^2(p-1)}{p-1}+O(u^2\sqrt{p}\,4^{\omega(p-1)})。$$

在 $u<\sqrt{p}$ 时为非平凡估计。

由此，证得定理2。

对导师张文鹏教授的指导深表谢意。

参 考 文 献

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

责任编辑 曹大刚

On Quadratic Residue Primitive Root and Problems of P. Gallapher's Type

Wu Shengli

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

Abstract By using transformation of trigonometric sum and estimates of certain character sum, two asymptotic formulas are given on the mean value of problems of P. Gallapher's type, involving quadratic residues and primitive roots.

Key words quadratic residue; primitive root; mean value; asymptotic formula; gallapher problem

·学术动态·

EI 收录陕西高校科技论文的统计

EI 即《工程论文索引》，是世界公认的工程技术领域的权威期刊。根据中国科技信息研究所公布的1991年～1995年我国高校国际科技论文排名榜，陕西高校统计如下。

表1 1991年～1995年EI收录的陕西省高校科技论文情况

我国院校排名位次	校名	篇数	理工类院校 名次	医学院校 名次	农林院校 名次	师范院校 名次
2	西安交通大学	758	2			
3	西北工业大学	679	3			
31	西安电子科技大学	174	31			
69	陕西师范大学	36				6
74	西北大学	32	68			
95	西安理工大学	22	83			
100	西安建筑科技大学	19	88			
114	西安工业学院	15	97			
118	西安公路交通大学	14	100			
124	西安石油学院	12	104			
150	第四军医大学	9		7		
190	西北纺织科技大学	5	149			
236	西北轻工业学院	3	180			
236	西北农业大学	3			3	
308	陕西工学院	1	217			
308	西安医科大学	1		29		
308	榆林师专	1				51

（薛 鲍）