Pure Mathematics 理论数学, 2020, 10(3), 167-171
Published Online March 2020 in Hans. http://www.hanspub.org/journal/pm
https://doi.org/10.12677/pm.2020.103024

Hans汉斯

Bounds for Double Exponential Sums and Its Application

Bo Chen

Sanda University, Shanghai
Email: bochen@sandau.edu.cn

Received: Feb. 20th, 2020; accepted: Mar. 6th, 2020; published: Mar. 13th, 2020

Abstract

Exponential sums play a key role in analytic number theory. In this paper, we establish bounds for double exponential sums by means of inequality and congruence. We then apply our estimate to obtain results on congruence equation.

Keywords

Exponential Sum, Exponential Functions, Congruence

二重指数和的边界及其应用

陈　波

上海杉达学院，上海
Email: bochen@sandau.edu.cn

收稿日期：2020年2月20日；录用日期：2020年3月6日；发布日期：2020年3月13日

摘　要

指数和在解析数论中扮演着非常重要的角色。在本文中，我们利用不等式以及同余等手段给出了二重指数和的边界，然后用该估计得到了有关于同余方程上的结果。

关键词

指数和，指数函数，同余

文章引用: 陈波. 二重指数和的边界及其应用[J]. 理论数学, 2020, 10(3): 167-171.
DOI: 10.12677/pm.2020.103024

1. 引言

设 r 是一个很大的整数，另设 g 是与 r 互质的整数且其模 r 的阶记为 T。给定两个连续的整数区间 $\mathrm{N}=\{u+1,u+2,\cdots,u+N\}$， $\mathrm{M}=\{v+1,v+2,\cdots,v+M\}$，其中 $N\le r$， $M\le T$，我们定义二重指数和

$$S_{a,r,g}(\mathrm{A},\mathrm{B};\mathrm{N},\mathrm{M})=\sum_{n\in\mathrm{N}}\sum_{m\in\mathrm{M}}\alpha_n\beta_m e_r\left(ang^m\right),$$

其中 $e_r(z)=\mathrm{e}^{2\pi\mathrm{i}z/r}$， α_n 和 β_m 都是复数且 $|\alpha_n|$， $|\beta_m|\le 1$。

当 r 为素数 p 时，Boyrgain [1]对于非常小的区间 N 和 M 估计了

$$S_{a,p,g}(\mathrm{N},\mathrm{M})=\sum_{n\in\mathrm{N}}\sum_{m\in\mathrm{M}}e_p\left(ang^m\right)$$

关于此方面的内容也可以参考[2]。最近，Shparlinski [3]和Garaev [4]分别得到了关于 $S_{a,p,g}(\mathrm{A},\mathrm{B};\mathrm{N},\mathrm{M})$ 的新的估计。

在本文中，我们主要给出 $S_{a,r,g}(\mathrm{A},\mathrm{B};\mathrm{N},\mathrm{M})$ 的边界，并由得到的结果给出同余方面的应用。文中会用到一些符号，例如 $A\ll B$ 表示存在常数 $c>0$ 使得 $|A|<cB$。另外， $A\prec B$ 表示 $|A|<r^{o(1)}B$。

2. 主要结果

定理 2.1：对于 $\forall a\in\mathrm{Z}_r^*$，我们有

$$S_{a,r,g}(\mathrm{A},\mathrm{B};\mathrm{N},\mathrm{M})<<r^{1/4}M^{3/4}N^{3/4}.$$

取 $r=p^2$，则可推导出如下结果。

定理 2.2：设 $\varepsilon>0$ 是一个很小的常数， N_i 和 M_i 是连续的整数区间且其阶满足

$$r\ge|\mathrm{N}_i|=N>r^{9/16+\varepsilon},\ |\mathrm{M}_i|=T>r^{1/2+\varepsilon},\ i=1,2,\cdots,6$$

那么对于任意整数 λ，同余方程

$$x_1g^{y_1}+x_2g^{y_2}+\cdots+x_6g^{y_6}\equiv\lambda(\mathrm{mod}\,r),\ x_i\in\mathrm{N}_i,\ y_i\in\mathrm{M}_i$$

的解的个数

$$\Delta=\frac{(NT)^6}{r}\left(1+O\left(r^{-\delta}\right)\right),\ \text{其中}\ \delta=\delta(\varepsilon)>0.$$

3. 引理

引理 3.1：当 $b\equiv 0(\mathrm{mod}\,r)$ 时， $\sum_{\lambda=0}^{r-1}e_r(b\lambda)=r$；否则其值为 0。

证明：当 $b\equiv 0(\mathrm{mod}\,r)$ 时，求和号中每项均为 1，因此和为 r；

反过来， $\sum_{\lambda=0}^{r-1}e_r(b\lambda)=\frac{1-e_r^r(b\lambda)}{1-e_r(b\lambda)}=0$。

证毕。

在 Bourgain [5]的定理 1 中取 $v=1$，我们得到

引理 3.2：设 Γ 是 Z_r^* 的一个子群。如果 $|\Gamma|>r^{1/2}$，那么对于任意正整数 h，同余方程 $ux_1\equiv x_2 \pmod r$，其中正整数 $x_1,x_2\le h$ 且 $u\in\Gamma$ 的解的个数

$$\Lambda \prec h|\Gamma|^{3/4} r^{-1/4}+h^2|\Gamma|r^{-1}.$$

推论 3.3：设 Γ 是 Z_r^* 的一个子群。如果 $|\Gamma|>r^{1/2}$，那么对于任意正整数 h，同余方程 $u_1x_1\equiv u_2x_2 \pmod r$，其中正整数 $x_1,x_2\le h$ 且 $u_1,u_2\in\Gamma$ 的解的个数

$$\Lambda_1 \prec h|\Gamma|^{7/4} r^{-1/4}+h^2|\Gamma|^2 r^{-1}.$$

结合 Garaev [4]中的引理 2，我们有

引理 3.4：设 $S_{a,r,g}(\mathrm{A},\mathrm{B};\mathrm{N},\mathrm{M})$ 中 $|\mathrm{N}|=N$，$|\mathrm{M}|=T$，那么同余方程

$$x_1g^{y_1}\equiv x_2g^{y_2} \pmod r,\quad x_1,x_2\in\mathrm{N},\quad y_1,y_2\in\mathrm{M}$$

的解的个数

$$J\prec T^2+NT^{7/4}r^{-1/4}+N^2T^2r^{-1}.$$

4. 定理 2.1 的证明

重新排列顺序并利用 Cauchy-Schwarz 不等式，我们有

$$\begin{aligned}\left|S_{a,r,g}(\mathrm{A},\mathrm{B};\mathrm{N},\mathrm{M})\right|^2 &\le \left(\sum_{m\in\mathrm{M}}|\beta_m|^2\right)\left(\sum_{m\in\mathrm{M}}\left|\sum_{n\in\mathrm{N}}\alpha_n e_r\left(ang^m\right)\right|\right)^2\\ &= M\sum_{m\in\mathrm{M}}\sum_{n_1,n_2\in\mathrm{N}}\alpha_{n_1}\overline{\alpha_{n_2}}e_r\left(ag^m(n_1-n_2)\right).\\ &\le M\sum_{n_1,n_2\in\mathrm{N}}\left|\sum_{m\in\mathrm{M}}e_r\left(ag^m(n_1-n_2)\right)\right|\end{aligned}$$

因此，如果我们定义 I_λ 为同余方程

$$n_1-n_2\equiv\lambda \pmod r,\quad n_1,n_2\in\mathrm{N}$$

的解的个数，那么

$$\left|S_{a,r,g}(\mathrm{A},\mathrm{B};\mathrm{N},\mathrm{M})\right|^2\le M\sum_{\lambda=0}^{r-1}I_\lambda\left|\sum_{m\in\mathrm{M}}e_r\left(ag^m\lambda\right)\right| \tag{1}$$

再次应用 Cauchy-Schwarz 不等式，我们得到

$$\sum_{\lambda=0}^{r-1}I_\lambda\left|\sum_{m\in\mathrm{M}}e_r\left(ag^m\lambda\right)\right|\le\left(\sum_{\lambda=0}^{r-1}I_\lambda^2\right)^{1/2}\left(\sum_{\lambda=0}^{r-1}\left|\sum_{m\in\mathrm{M}}e_r\left(ag^m\lambda\right)\right|^2\right)^{1/2} \tag{2}$$

然而，因为 $n_1,n_2\in\mathrm{N}$，所以我们有

$$\sum_{\lambda=0}^{r-1}I_\lambda^2<<1^2+2^2+\cdots+N^2<<N^3 \tag{3}$$

另一方面，

$$\begin{aligned}\sum_{\lambda=0}^{r-1}\left|\sum_{m\in\mathrm{M}}e_r\left(ag^m\lambda\right)\right|^2 &= \sum_{\lambda=0}^{r-1}\sum_{m_1\in\mathrm{M}}e_r\left(ag^{m_1}\lambda\right)\overline{\sum_{m_2\in\mathrm{M}}e_r\left(ag^{m_2}\lambda\right)}\\ &= \sum_{m_1,m_2\in\mathrm{M}}\sum_{\lambda=0}^{r-1}e_r\left(a\left(g^{m_1}-g^{m_2}\right)\lambda\right)\end{aligned}.$$

由引理 3.1，当 $g^{m_1}-g^{m_2}\equiv 0\left(\mathrm{mod}\, r\right)$ 时，$\sum_{\lambda=0}^{r-1}e_r\left(a\left(g^{m_1}-g^{m_2}\right)\lambda\right)=r$；否则其值为 0。

所以

$$\sum_{\lambda=0}^{r-1}\left|\sum_{m\in \mathrm{M}}e_r\left(ag^m\lambda\right)\right|^2=Mr. \tag{4}$$

将(3)和(4)代入(2)，得

$$\sum_{\lambda=0}^{r-1}I_\lambda\left|\sum_{m\in \mathrm{M}}e_r\left(ag^m\lambda\right)\right|<<N^{3/2}M^{1/2}r^{1/2}.$$

再将其代入(1)，我们便有

$$\left|S_{a,r,g}\left(\mathrm{A},\mathrm{B};\mathrm{N},\mathrm{M}\right)\right|^2<<M^{3/2}N^{1/2}r^{1/2}.$$

因此，定理 2.1 得证。

5. 定理 2.2 的证明

首先，我们将 Δ 改写为

$$\Delta=\frac{1}{r}\sum_{a=0}^{r-1}\prod_{j=1}^{6}\left(\sum_{x\in \mathrm{N}_j}\sum_{y\in \mathrm{M}_j}e_r\left(axg^y\right)\right)e_r\left(-a\lambda\right). \tag{5}$$

当 $r=p^2$ 时，若 $\gcd\left(a,r\right)\neq 1$，则定理 2.1 证明中的(4)为

$$\sum_{\lambda=0}^{r-1}\left|\sum_{m\in \mathrm{M}}e_r\left(ag^m\lambda\right)\right|^2\le Mr+r^{1/2}V$$

其中 V 为同余方程

$$g^{m_1}-g^{m_2}\equiv 0\left(\mathrm{mod}\, r^{1/2}\right),\ m_1,m_2\in \mathrm{M}$$

的解的个数。

因此，

$$\sum_{\lambda=0}^{r-1}\left|\sum_{m\in \mathrm{M}}e_r\left(ag^m\lambda\right)\right|^2<<Mr.$$

从而对于正整数 a，我们恒有

$$S_{a,r,g}\left(\mathrm{A},\mathrm{B};\mathrm{N},\mathrm{M}\right)<<r^{1/4}M^{3/4}N^{3/4}.$$

在(5)中，将 $a=0$ 的项分离，并利用上述结果，我们有

$$\left|\Delta-\frac{1}{r}\prod_{j=1}^{6}\left(NT\right)\right|<W\prod_{j=1}^{4}\left(r^{1/4+\delta_0}N^{3/4}T^{3/4}\right)\le W\prod_{j=1}^{4}\frac{NT}{r^{1/64+\delta_1}} \tag{6}$$

其中 $0<\delta_0<\frac{\varepsilon}{2}$，$\delta_1>0$ 且

$$W=\frac{1}{r}\sum_{a=1}^{r-1}\left|\sum_{x\in \mathrm{N}_5}\sum_{y\in \mathrm{M}_5}e_r\left(axg^y\right)\right|\left|\sum_{x\in \mathrm{N}_6}\sum_{y\in \mathrm{M}_6}e_r\left(axg^y\right)\right|.$$

利用 Cauchy-Schwarz 不等式，我们得到

$$W \le \sqrt{\frac{1}{r}\sum_{a=0}^{r-1}\left|\sum_{x\in \mathrm{N}_5}\sum_{y\in \mathrm{M}_5} e_r\left(axg^{y}\right)\right|^2}\sqrt{\frac{1}{r}\sum_{a=0}^{r-1}\left|\sum_{x\in \mathrm{N}_6}\sum_{y\in \mathrm{M}_6} e_r\left(axg^{y}\right)\right|^2} = \sqrt{T_5}\sqrt{T_6} \tag{7}$$

其中 T_i 是同余方程

$$x_1 g^{y_1} \equiv x_2 g^{y_2} \left(\mathrm{mod}\, r\right),\ \ x_1, x_2 \in \mathrm{N}_i,\ \ y_1, y_2 \in \mathrm{M}_i$$

的解的个数。

由引理 3.4，我们有

$$T_i \prec N^2T^2\left(\frac{1}{N^2}+\frac{1}{NT^{1/4}r^{1/4}}+\frac{1}{r}\right) < \frac{N^2T^2}{r^{15/16+\delta_2}},\ \text{其中}\ \delta_2 > 0.$$

将其代入(7)，得

$$W \le \frac{N^2T^2}{r^{15/16+\delta_3}},\ \text{其中}\ \delta_3 > 0.$$

代入(6)，我们有

$$\left|\Delta - \frac{1}{r}\prod_{j=1}^{6}\left(NT\right)\right| < \frac{1}{r^{1+\delta}}\prod_{j=1}^{6}\left(NT\right),\ \text{其中}\ \delta > 0.$$

证毕。

致　谢

感谢 M. Z. Garaev 的文章给我的思路，以及同事们对我工作的支持。

参考文献

[1] Bourgain, J. (2009) On the Distribution of the Residues of Small Multiplicative Subgroups of F_p. *Israel Journal of Mathematics*, **172**, 61-74. https://doi.org/10.1007/s11856-009-0063-4

[2] Hegyvari, N. and Hennecart, F. (2012) Distribution of Residues in Approximate Subgroups of F_p^*. *Proceedings of the American Mathematical Society*, **140**, 1-6. https://doi.org/10.1090/S0002-9939-2011-10866-9

[3] Shparlinski, I.E. and Yau, K.H. (2017) Double Exponential Sums with Exponential Functions. *International Journal of Number Theory*, **13**, 2531-2543. https://doi.org/10.1142/S179304211750141X

[4] Garaev, M.Z. (2019) Double Exponential Sums and Congruences with Intervals and Exponential Functions Modulo a Prime. *Journal of Number Theory*, **199**, 377-388. https://doi.org/10.1016/j.jnt.2018.11.019

[5] Bourgain, J., Konyagin, S.V. and Shparlinski, I.E. (2008) Product Sets of Rationals, Multiplicative Translates of Subgroups in Residue Rings, and Fixed Points of the Discrete Logarithm. *International Mathematics Research Notices*, 1 p.