第13卷 第1期 曲阜师范大学学报 Vol.13 No.1
1987年1月 Journal of Qufu Normal University Jan. 1987

再论某一类指数方幂和的同余问题

方 玉 光

提 要

本文给出一类指数方幂和的同余问题一个定理。

§1. 引言

设$S_r(\Pi, d)$表示mod n的一简化剩余系中指数为d的元素的r次方幂和。C.F.Gauss〔3〕证明了 $S_1(p, p-1)\equiv\mu(p-1)(\mathrm{mod}\,p)$；1830年，M. A. Stern〔4〕证明了 $S_1(p, d)\equiv\mu(d)(\mathrm{mod}\,p)$；1883年，A. R. Forsyth〔5〕给出了$S_r(p, p-1)$的同余定理，但其结果比较复杂；1952年，R. Moller〔2〕证明了$S_r(p, d)\equiv\frac{\varphi(d)}{\varphi(d_1)}\mu(d_1)(\mathrm{mod}\,p)$ 其中$d_1=d/(r,d)$，H. S. Zuckerman在〔2〕之后作一注记，给出了Moller定理的另一简单证明。H. Gupta在〔1〕中又给出了Moller定理的一个证明，本文作者在〔6〕中证明了$S_r(p^\alpha, d)\equiv\frac{\varphi(d)}{\varphi(l_0)}\mu(l_0)(mod\,p^\alpha)$，其中$d/(r, d)=p^{r_0}l_0$，$p\nmid l_0$，$p$为奇素数。

本文证明了

定理 $S_r(2,1)\equiv1(\mathrm{mod}2)$，$S_r(4,2)\equiv(-1)^r(\mathrm{mod}4)$，当$\alpha\geq3$，$0<n_0\leq\alpha-2$时，$S_r(2^\alpha, 2^{n_0})\equiv(-1)^r\Delta(n_0)+[1+(-1)^r]\varphi(2^{n_0})(\mathrm{mod}2^\alpha)$。

其中 $\Delta(n_0)=\left[\frac{1}{n_0}\right]=\begin{cases}1 & \text{当}n_0=1\text{时}\\ 2 & \text{当}n_0>1\text{时}\end{cases}$

§2. 定理的证明

很容易得到 $S_r(2,1)\equiv1(\mathrm{mod}2)$，$S_r(4,2)\equiv(-1)^r(\mathrm{mod}4)$。

当$\alpha\geq3$时，5的指数(关于mod2^α)为$2^{\alpha-2}$。且$\pm5^0, \pm5^1, \pm5^2, \cdots \pm5^{2^{\alpha-2}-1}$构成mod$2^\alpha$的一个简化剩余系（见〔7〕）。

A Note on Independency

Luo Qiao-lin
(Institute of Systems Science, Academia Scinica)

Abstract

This paper gives the necessary and sufficient condition for that continuous model accidental vectors with arbitrarily partial vectors independent each other but all dependent have united discribution density.

下面分两种情况证明

（i）当$n_0=1$时，若n的指数为2，则$(n,2)=1$，且存在ν，ν_0，使

$$n\equiv(-1)^{\nu}5^{\nu_0}(\bmod 2^{\alpha})$$

则由$n^2\equiv1(\bmod 2^{\alpha})$得：$2^{\alpha-3}\mid\nu_0$，故只有$-1$，$\pm5^{2^{\alpha-3}}$的指数为2，故

$$S_1(2^{\alpha},2)=(-1)^{\nu}+[1+(-1)^{\nu}]5^{2^{\alpha-3}\nu_0}\equiv\begin{cases}-1(\bmod 2^{\alpha}) & \text{当}2\nmid\nu\text{时}\\ 3(\bmod 2^{\alpha}) & \text{当}2\mid\nu\text{时}\end{cases}$$

$$\equiv1+2(-1)^{\nu}(\bmod 2^{\alpha}).$$

（ii）当$n_0>1$时，设n的指数为2^{n_0}，$n\equiv(-1)^{\nu}5^{\nu_0}(\bmod 2^{\alpha})$．则由$n^{2^{n_0}}\equiv1(\bmod 2^{\alpha})$可得$2^{\alpha-n_0-2}\mid\nu_0$，且由指数的最小性易知$2^{\alpha-n_0-2}\|\nu_0$（$p^{r}\|m$表示$p^{r}\mid m$，但$p^{r+1}\nmid m$）．进而$\{(-1)^{\nu}5^{\nu_0}\mid\nu=0,1,2^{\alpha-n_0-2}\|\nu_0\}$构成mod$2^{\alpha}$一简化剩余系中指数为$2^{n_0}$的所有元素．记$l=r\cdot2^{\alpha-n_0-2}$并应用〔1〕中引理2有：

$$S(2^{\alpha},2^{n_0})=\sum_{\substack{\nu_0:2^{\alpha-n_0-2}\|\nu_0\\ \nu=0,1}}[(-1)^{\nu}5^{\nu_0}]^{r}=[1+(-1)^{r}]\sum_{\nu_0:2^{\alpha-n_0-2}\|\nu_0}5^{r\nu_0}$$

$$=[1+(-1)^{r}]\sum_{k=1}^{2^{n_0}}(5^{l})^{k}$$

$$=[1+(-1)^{r}]\sum_{d\mid2^{n_0}}\mu(d)\left(\sum_{k=1}^{2^{n_0}/d}(5^{l})^{kd}\right)$$

$$=[1+(-1)^{r}]\sum_{d\mid2^{n_0}}\mu(d)\frac{5^{l\cdot2^{n_0}}-1}{5^{ld}-1}\cdot5^{ld}$$

$$=[1+(-1)^{r}]\left(\mu(1)\frac{5^{l\cdot2^{n_0}}-1}{5^{l}-1}5^{l}+\mu(2)\frac{5^{l\cdot2^{n_0}}-1}{5^{2l}-1}\cdot5^{2l}\right)$$

$$=[1+(-1)^{r}]\frac{5^{l\cdot2^{n_0}}-1}{5^{2l}-1}\cdot5^{l}\qquad(1)$$

当$2\nmid r$时，$S_1(2^{\alpha},2^{n_0})\equiv0(\bmod 2^{\alpha})$．

当$2\mid r$时，讨论其同余情况。

很容易由数学归纳法证明

$$5^{2^{l-2}}\equiv1+2^{l}(\bmod 2^{l+1})\quad\text{其中}2\le l\le\alpha-1.$$

故必有 $5^{2^{\alpha-n_0-2}}\equiv1+2^{\alpha-n_0}(\bmod 2^{\alpha-n_0+1})$，当$2\mid r$时，

$5^{r\cdot2^{\alpha-n_0-2}}\equiv1+2^{r_0}(\bmod 2^{r_0+1})$，即$5^{l}\equiv1+2^{r_0}(\bmod 2^{r_0+1})$，其中$r_0\ge\alpha-n_0+1$，设$5^{l}=1+\mu2^{r_0}$，$(2\nmid\mu)$，则有：

$$5^{2l}=1+\mu_1 2^{r_0+1}\qquad(2\nmid\mu_1).$$

于是 $\dfrac{5^{l\cdot2^{n_0}}-1}{5^{2l}-1}=\dfrac{(1+\mu_1 2^{r_0+1})^{2^{n_0-1}}-1}{\mu_1 2^{r_0+1}}=2^{r_0-1}+2^{r_0-1}\sum_{k=2}\binom{2^{n_0-1}}{k}\times\mu_1^{k-1}2^{k(r_0-1)}$

$$\equiv2^{r_0-1}(\bmod 2^{\alpha}).$$

其中用到了$pot_2\left(\binom{2^{n_0-1}}{k}2^{k(r_0-1)}\right)\ge\alpha+r_0+1\quad(k\ge2)$．进而有：

$\dfrac{5^{l\cdot2^{n_0}}-1}{5^{2l}-1}\cdot5^{l}\equiv2^{r_0-1}+\mu2^{r_0-1}(\bmod 2^{\alpha})\equiv2^{r_0-1}(\bmod 2^{\alpha})$ 代入（1）得：

$S_r(2^\alpha, 2^{n_0}) \equiv [1+(-1)^r]2^{n_0-1} \pmod{2^\alpha} \equiv [1+(-1)^r]\varphi(2^{n_0}) \pmod{2^\alpha}$.

综合 (i) (ii) 可得

$$S_r(2^\alpha, 2^{n_0}) \equiv \Delta(n_0)(-1)^r + [1+(-1)^r]\varphi(2^{n_0}) \pmod{2^\alpha}$$

参 考 文 献

〔1〕 Gupta, H. Selected Topics in Number Theory. ABACUS Press, 1980.

〔2〕 Moller, R. Sums of powers of number having a given exponent modulo a prime. Amer. Math. Monthly 59(1952)

〔3〕 Gauss, C. F. Disquisitions Arithmeticae, arts. 80—81.

〔4〕 Stern, M. A. Bemerkungen über hohere Arithmetrik. Journal für Mathematick, Vol. VI. (1830) p. p. 147—153.

〔5〕 Forsyth, A. R. primitive roots of primes and their residnes, Messenger of Mathematics, Vol. XII(1883—4) pp. 180—185.

〔6〕 方玉光，某一类指数方幂和的同余问题，数学研究与评论（待发）.

〔7〕 Ireland, k. & Rosen, M. A Classical Introduction to Modern Number Theory. Springer-Verlag, New York-Heidelberg-Berlin, 1982.

Second on the Same Remainder problem of a Class of Exponential Sum of powers

Fang Yu-guang

Abstract

In this paper, a theorem of the same remainder of a class of exponential sum of powers is given.