若干数论问题的注记①

单 增
(数学系)

摘要 本文主要对几个与同余类有关的命题给出新的简化证明.

关键词 代数数域，理想，完系，缩系.

(一)

张树生在[1]中证明了

定理. 对一切素数$p \geqslant 5$,

$$\sum_{k=1}^{p-1} \frac{1}{tp+k} \equiv 0 \pmod{p^2} \tag{1}$$

其中t为任一整数.

他认为这个定理推广了华罗庚《数论导引》第二章 § 10 的 Wolstenholme 定理.

张的证明比较复杂. 其实华罗庚书中的证法稍作修改即可得出 (1): 命

$$\prod_{k=1}^{p-1}(x-(tp+k)) = x^{p-1} - s_1 x^{p-2} + \cdots + s_{p-1} \tag{2}$$

因

$$\prod_{k=1}^{p-1}(x-(tp+k)) \equiv x^{p-1} - 1 \pmod{p}$$

所以

$$p \mid (s_1, s_2, \cdots, s_{p-2}) \tag{3}$$

在(2)中令$x = (2t+1)p$, 则

$$\prod_{k=1}^{p-1}(tp+p-k) = ((2t+1)p)^{p-1} - s_1((2t+1)p)^{p-2} + \cdots + s_{p-1}$$

即

$$0 = ((2t+1)p)^{p-2} - s_1((2t+1)p)^{p-3} + \cdots - s_{p-2}$$

结合(3)得

$$s_{p-2} \equiv 0 \pmod{p^2}$$

即

$$p^2 \mid \left(\prod_{k=1}^{p-1}(tp+k) \cdot \sum_{k=1}^{p-1} \frac{1}{tp+k} \right)$$

亦即(1)式成立.

---

①本文于1991年1月2日收到.

〈二〉

设 $S_{r(n,d)}$ 表示 mod$n$ 的缩系中指数为 d 的元素的 r 次方幂和 .1952 年 R.Moller[2] 将 Gauss 等人的古典结果[3],[4]

$$S_{1(p,\ p-1)} \equiv \mu(p-1)(\mathrm{mod}p),$$

$$S_1(p,\ d) \equiv \mu(d)(\mathrm{mod}p),$$

推广为

$$S_{r(p,\ d)} \equiv \frac{\varphi(d)}{\varphi(d_1)}\mu(d_1)(\mathrm{mod}p) \tag{4}$$

其中 $d_1 = \dfrac{d}{(r,d)}$

1980 年，H.Gupta[3] 给出 (4) 的一个简化证明 .1987 年方玉光[6] 又将 (4) 推广为

$$S_r(p^\alpha,d) \equiv \frac{\varphi(d)}{\varphi(l_0)}\mu(l_0)(\mathrm{mod}p^\alpha), \tag{5}$$

其中l_0定义如下:

$$d_1 = \frac{d}{(r,\ d)} = p^m l_0,\ \ p\nmid l_0. \tag{6}$$

在这里我们给出 (5) 的一个简短的新证明 .

引理 设 g 为 modp^α 的原根，则对 $0 \leqslant m < \alpha$,

$$\sum_{h=1}^{p^m} g^{\varphi(p^\alpha)rh/p^m} \equiv p^m(\mathrm{mod}p^\alpha) \tag{7}$$

证明 对α进行归纳.

$\alpha = 1$ 时，$m = 0$.(7) 即 Fermat 小定理 .

假设命题对于 $\alpha - 1(\geqslant 1)$ 成立 . 则对 $0 \leqslant m < \alpha$,

$$\sum_{h=1}^{p^m} g^{\varphi(p^\alpha)rh/p^m} = \sum_{h=1}^{p^m} g^{\varphi(p^{\alpha-1})rh/p^{m-1}} = \sum_{k=0}^{p-1}\sum_{h=1}^{p^{m-1}} g^{\varphi(p^{\alpha-1})r(h+kp^{m-1})/p^{m-1}}$$

$$= \sum_{h=1}^{p^{m-1}} g^{\varphi(p^{\alpha-1})rh/p^{m-1}} \cdot \sum_{k=0}^{p-1} g^{\varphi(p^{\alpha-1})rk} \tag{8}$$

由归纳假设，(8)的前一个因子为$p^{m-1} + a \cdot p^{\alpha-1}$.由Euler定理,

$$g^{\varphi(p^{\alpha-1})} = 1 + bp^{\alpha-1}$$

所以

$$\sum_{h=1}^{p^m} g^{\varphi(p^\alpha)rh/p^m} = (p^{m-1} + ap^{\alpha-1}) \cdot \sum_{k=0}^{p-1}(1 + bp^{\alpha-1})^{rk}$$

$$= (p^{m-1} + ap^{\alpha-1})\sum_{k=0}^{p-1}(1 + brkp^{\alpha-1} + \cdots)$$

$$= (p^{m-1} + ap^{\alpha-1})(p + br \cdot p^{\alpha-1} \cdot \frac{p(p-1)}{2} + \cdots)$$

$$\equiv p^{m} \pmod{p^{\alpha}}.$$

因此引理成立.

设 $r_1 = \frac{r}{(d, r)}$，由于 $h \equiv h' (\mathrm{mod} d_1)$ 时，

$$g^{\frac{\varphi(p^{\alpha})r_1 h}{d_1}} \equiv g^{\frac{\varphi(p^{\alpha})r_1 h'}{d_1}} \pmod{p^{\alpha}}$$

所以

$$S_{r(p^{\alpha},d)} = \sum_{h(\mathrm{mod}d)}^{*} g^{\frac{\varphi(p^{\alpha})rh}{d}} = \sum_{h(\mathrm{mod}d)}^{*} g^{\frac{\varphi(p^{\alpha})r_1 h}{d_1}}$$

$$\equiv \frac{\varphi(d)}{\varphi(d_1)} \sum_{h(\mathrm{mod}d_1)}^{*} g^{\frac{\varphi(p^{\alpha})r_1 h}{d_1}} \pmod{p^{\alpha}} \tag{9}$$

而

$$\sum_{h(\mathrm{mod}d_1)}^{*} g^{\frac{\varphi(p^{\alpha})r_1 h}{d_1}} = \sum_{h(\mathrm{mod}d_1)} g^{\frac{\varphi(p^{\alpha})r_1 h}{d_1}} \sum_{s \mid (h, d_1)} \mu(s) = \sum_{s \mid d_1} \mu(s) \sum_{h(\mathrm{mod}\frac{d_1}{s})} g^{\frac{\varphi(p^{\alpha})r_1 hs}{d_1}}$$

$$= \sum_{s \mid p^{m}} \mu(s) \sum_{t \mid l_0} \mu(t) \sum_{h(\mathrm{mod}\frac{p^{m} l_0}{st})} g^{\frac{\varphi(p^{\alpha})r_1 hst}{p^{m} l_0}} = \sum_{s \mid p} \mu(s) \sum_{t \mid l_0} \mu(t) \sum_{h(\mathrm{mod}\frac{p^{m} l_0}{st})} g^{\frac{\varphi(p^{\alpha})r_1 hst}{p^{m} l_0}}$$

其中最里面的和，在 $t \neq l_0$ 时，值为

$$\frac{g^{\varphi(p^{\alpha})r_1 \cdot \frac{st}{p^{m} l_0} \cdot \frac{p^{m} l_0}{st}} - 1}{g^{\varphi(p^{\alpha})r_1 \cdot \frac{st}{p^{m} l_0}} - 1} \equiv 0 \pmod{p^{\alpha}}$$

在 $t = l_0$ 时，值为

$$\sum_{h(\mathrm{mod}\frac{p^{m}}{s})} g^{\varphi(p^{\alpha})r_1 hs / p^{m}}$$

因此

$$\sum_{h(\mathrm{mod}d_1)}^{*} g^{\varphi(p^{\alpha})r_1 h / d_1} = \sum_{s \mid p} \mu(s)\mu(l_0) \sum_{h(\mathrm{mod}\frac{p^{m}}{s})} g^{\varphi(p^{\alpha})r_1 hs / p^{m}}$$

$$= \mu(l_0)\left(\sum_{h(\mathrm{mod}p^{m})} g^{\varphi(p^{\alpha})r_1 h / p^{m}} - \sum_{h(\mathrm{mod}p^{m-1})} g^{\varphi(p^{\alpha})r_1 h / p^{m-1}} \right)$$

由(7)

$$\equiv \mu(l_0)(p^{m} - p^{m-1}) \pmod{p^{\alpha}}$$

$$\equiv \mu(l_0) \cdot \frac{\varphi(d_1)}{\varphi(l_0)} \pmod{p^{\alpha}} \tag{10}$$

由 (9)，(10)，

$$S_r(p^{\alpha}, d) \equiv \frac{\varphi(d)}{\varphi(d_1)} \cdot \mu(l_0) \cdot \frac{\varphi(d_1)}{\varphi(l_0)} \equiv \frac{\varphi(d)}{\varphi(l_0)} \mu(l_0) \pmod{p^{\alpha}}.$$

当 $m=0$ 时，由 $d_1=l_0$ 及上面推导过程容易看出 (5) 式仍然成立.

(三)

设 M 为某代数数域中的整理想，$M\neq 0$、1，M†2，

$$\alpha_1,\ \alpha_2,\ \cdots\alpha_n \tag{11}$$

与

$$\beta_1,\ \beta_2,\ \cdots,\ \beta_n \tag{12}$$

为 modM 的两个完全剩余系，其中 $n=N(M)$. 旷京华等[7] 曾证明积

$$\alpha_1\beta_1,\ \alpha_2\beta_2,\ \cdots,\ \alpha_n\beta_n \tag{13}$$

不是 modM 的完系. 我们在这里另给一个证明:

若 (13) 是 modM 的完系，不妨设前面 $\varphi(M)=t$ 个是 modM 的缩系，这时 $\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_t$ 与 $\beta_1,\ \beta_2,\ \cdots,\ \beta_t$ 也必然是 modM 的缩系.

设素理想 $N|M$，若 $(\alpha_t\beta_t,\ M)=P$，则由于 α_t、β_t 均不在 modM 的缩系中，必有 $P|\alpha_t$，$P|\beta_t$ 并且 $P\|M$，于是可设 $M=\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_m$，其中 $\mathfrak{p}_i(1\leqslant i\leqslant m)$ 为不同的素理想.

用归纳法易知当且仅当 $(\alpha_t,\ M)=(\beta_t,\ M)=\mathfrak{p}_{j_1}\mathfrak{p}_{j_2}\cdots\mathfrak{p}_{j_s}$ 时，$(\alpha_t\beta_t,\ M)=\mathfrak{p}_{j_1}\mathfrak{p}_{j_2}\cdots\mathfrak{p}_{j_s}$，并且这样的 i 恰有 $\varphi\left(\dfrac{M}{\mathfrak{p}_{j_1}\mathfrak{p}_{j_2}\cdots\mathfrak{p}_{j_s}}\right)$ 个.

特别地，设 α_{t_1}、α_{t_2}、$\cdots$、α_{t_k} 及 β_{t_1}、β_{t_2}、$\cdots$、β_{t_k} 满足 $(\alpha_{t_1},\ M)=\cdots=(\alpha_{t_k},\ M)=(\beta_{t_1},\ M)=\cdots=(\beta_{t_k},\ M)=\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_{m-1}$，其中 $k=\varphi(\mathfrak{p}_m)$，则 $(\alpha_{t_1}\beta_{t_1},\ M)=\cdots=(\alpha_{t_k}\beta_{t_k},\ M)=\mathfrak{p}_1\mathfrak{p}_2\cdots\mathfrak{p}_{m-1}$.

由于 $\alpha_{t_1},\ \cdots,\ \alpha_{t_k}$ 是 modM 的不同的剩余类，所以 $\alpha_{t_1},\ \cdots\alpha_{t_k}$ 是 mod$\mathfrak{p}_m$ 的不同的剩余类，同样 $\beta_{t_1},\ \cdots\beta_{t_k}$ 及 $\alpha_{t_1}\beta_{t_1},\ \cdots\alpha_{t_k}\beta_{t_k}$ 也都是 mod$\mathfrak{p}_m$ 的不同剩余类，于是它们均为 mod$\mathfrak{p}_m$ 的缩系. 由 Wilson 定理，

$$\alpha_{t_1}\alpha_{t_2}\cdots\alpha_{t_k}\equiv -1\pmod{\mathfrak{p}_m}$$

$$\beta_{t_1}\beta_{t_2}\cdots\beta_{t_k}\equiv -1\pmod{\mathfrak{p}_m}$$

$$(\alpha_{t_1}\beta_{t_1})(\alpha_{t_2}\beta_{t_2})\cdots(\alpha_{t_k}\beta_{t_k})\equiv -1\pmod{\mathfrak{p}_m}$$

但将前两个式子相乘所得结果与第三个式子矛盾，这表明 (13) 不是 modM 的完系.

〈四〉

旷京华[7] 证明了以下定理.

定理 设 A 为代数数域 K 中的理想，$B=(2,\ A)$，并且 $N(B)=2$. 若 $n=N(A)$，

$$\alpha_1,\ \alpha_2,\ \cdots,\ \alpha_n \tag{14}$$

与

$$\beta_1,\ \beta_2,\ \cdots\beta_n \tag{15}$$

是 modA 的两组完全剩余系，则

$$\alpha_1+\beta_1,\ \alpha_2+\beta_2,\ \cdots\alpha_n+\beta_n \tag{16}$$

不是 modA 的完全剩余系.

这定理显然是从 $K=Q$ 时相应的命题推广而来．我们的证明如下:

因为 $N(\mathbf{B})=2$，所以 B 是素理想，设

$$\mathbf{A}=\mathbf{B}^a\mathbf{N},$$

$$(2)=\mathbf{B}^b\mathbf{M}$$

其中 M、N、B 两两互素；$a\geqslant 1$，$b\geqslant 1$ 并且至少有一个为 1.

由于 $-\alpha_1$，$-\alpha_2$，$\cdots-\alpha_n$ 也是 modA 的完系，所以

$$\sum(\alpha_i+\beta_i)\equiv\sum(\alpha_i+(-\alpha_i))\equiv 0\pmod{\mathrm{A}} \tag{17}$$

另一方面，对 modA 的任一完系 (14)，考虑和 $\sum\alpha_i(\mathrm{modA})$，将其中形如 α_i 与 $\alpha_i'\equiv-\alpha_i(\mathrm{modA})$ 的两项互相抵消，只剩下满足

$$\alpha_i\equiv-\alpha_i(\mathrm{modA}) \tag{18}$$

的那些 α_i.

(18) 即 $\mathbf{B}^a\mathbf{N}|(2\alpha_i)$，从而 $\mathbf{B}^a\mathbf{N}|\mathbf{B}^b\mathbf{M}(\alpha_i)$．由于 M、N、B 两两互素，不论 $a=1$ 或 $b=1$，均有

$$\mathbf{B}^{a-1}\mathbf{N}|(\alpha_i)$$

由于 $N(\mathbf{A})\div N(\mathbf{B}^{a-1}N)=N(\mathbf{B})=2$，所以恰有两个 α_i 满足 (18)．其中一个当然是 $\alpha_i\equiv 0(\mathrm{modA})$，另一个 $\alpha_i\not\equiv 0(\mathrm{modA})$，这样，对 modA 的任一完系 (14)，

$$\sum\alpha_i\not\equiv 0(\mathrm{modA}).$$

因而，由 (17) 即知结论成立.

参考文献

1 张树生.一个数论定理的推广.数学的实践与认识，1989；1：86–91

2 Moller.R.Sums of powers of number having a Given Exponent Modular a Prime.Amer Monthly.1952；59：180–182

3 Gauss C. Disquisitions Arithmeticae arts.80–81

4 Stern M. Bemerkungen über Hohere Arithmetrik Journal für Mathmetick. 1830；6：180–185

5 Gupta H.Selected Topics in Namber Theory.ABACUS Press，1980；56–57

6 方玉光.再论某一类指数幂和的同余问题．曲阜师范大学学报，1987；72–75

7 旷京华，万大庆．关于覆盖剩余类的注记．数论研究与评论，1984；4：1

Notes on Some Problems in Number Theory

Shan Zun

(Department of Mathematics)

Abstract We give some new neat proofs of propositions about residue systems.

Key words Algebraic fields, Ideal, Complete residue system, Reduced residue system.

(上接第 25 页)

证明 只需重证 x_* 是 $\{T_i\}$ 的公共不动点，具体可仿照文〔1〕定理 5 的证明，从略。

注 4 定理 2.2 是文〔1〕定理 5 的修正，在定理 2.2 中令 $\triangle = \mathrm{Min}$，$\varphi(t) = t/k$（其中 $k \in (0, 1)$ 是常数），即得〔4〕的定理 2.1。

参考文献

1 方锦暄.数学年刊，1990；11A(6)：707-711

2 Schweizer, B., Sklar, A., Probabilistic Metric Spaces, North-Holland, 1983

3 Hadzic, O., Mat. Vesnik, 1979; 3(16)(31): 125-133

4 Zhang Shisheng. Acta Math. Sinica, New Series, 1985; 1(4): 366-377

On Some Fixed Point Theorems in Menger Spaces

Fang Jinxuan

(Department of Mathematics)

Abstract In this paper, several fixed point theorems for single-valued and multi-valued mappings in Menger spaces are given. We further generalize Theorem 1 and Theorem 2 in 〔1〕, and make an appropriate correction to Theorem 4 (Theorem 5) in 〔1〕.

key words Menger space, h-type t-norm, single-valued (multi-valued) mapping, fixed point.