

Dedekind 整环中的完全剩余系*

高 维 东

(东北师大数学系,长春 130024)

关于有理整数的完全剩余系,Vijayahavan 和 Chowla 在 1988 年得到一个优美的结果:

定理 A^[1]. 设 $q > 2, r_1, \dots, r_q$ 和 s_1, \dots, s_q 是模 q 的两个完全剩余系.

1954 年 Coles 和 Olson^[2] 给出了简化证明. 1987 年孙琦和旷京华^[3]把上述结果推广到了任意有限次代数数域的代数整数环上而得到:

定理 B 对 $A \neq p_1, \dots, p_k$, 诸 p_j 是 2 的某些不同的素理想因子, 且 A 非单位理想, 若 $\alpha_1, \dots, \alpha_{N(A)}$ 和 $\beta_1, \dots, \beta_{N(A)}$ 是 A 的任意两组完全剩余系, 则有 $\alpha_1\beta_1, \dots, \alpha_{N(A)}\beta_{N(A)}$ 不是 A 的完全剩余系.

本文将上述结果推广到了 Dedekind 整环上, 所得结果包含了定理 A 和定理 B.

定理 设 R 为 Dedekind 整环, A 为 R 的理想, $A \neq R, R/A$ 为有限环, 且 $A \neq p_1, \dots, p_s$ (诸 p_i 为不同的素理想, 且域 R/p_i 之特征均为 2); 设 s 为一正偶数, 则 A 的任 s 个完全剩余系(参见[3]), $a_1^{(i)}, \dots, a_N^{(i)} (1 \leq i \leq s, N = |R/A|)$ 都使得 $\prod_{i=1}^s a_i^{(i)}, \dots, \prod_{i=1}^s a_N^{(i)}$ 不是 A 的完全剩余系.

引理 设 F_q 为 q 阶有限域, $2 \nmid q$, 则对 F_q 的任 $s(2 \mid s)$ 个置换 $a_1^{(i)}, \dots, a_s^{(i)} (1 \leq i \leq s)$ 有 $\prod_{i=1}^s a_1^{(i)}, \dots, \prod_{i=1}^s a_s^{(i)}$ 不为 F_q 的置换.

证明 用反证法. 假设存在 F_q 的 s 个置换 $a_1^{(i)}, \dots, a_s^{(i)} (1 \leq i \leq s)$ 使得 $\prod_{i=1}^s a_1^{(i)}, \dots, \prod_{i=1}^s a_s^{(i)}$ 也为 F_q 之一置换. 显见, 不妨设 $a_1^{(1)} = a_1^{(2)} = \dots = a_1^{(s)} = 0$, 设 θ 为 F_q 的一生成元, 则 $a_i^{(i)} = \theta^{a_i^{(i)}}$, 且 $n_1^{(1)}, \dots, n_{q-1}^{(1)}$ 成为 $q-1$ 的一个完全剩余系, 于是 $\prod_{i=1}^s n_1^{(1)}, \dots, \prod_{i=1}^s n_{q-1}^{(1)}$ 为 $q-1$ 一完全剩余系. 从而有

$$\begin{aligned}\frac{q-1}{2} &\equiv 0 + \frac{q-1}{2} + \sum_{i=1}^{\frac{s-2}{2}} (i - q - 1 - i) \equiv \sum_{j=1}^{\frac{s-1}{2}} \sum_{i=1}^s n_j^{(i)} \\ &\equiv \sum_{i=1}^s \sum_{j=1}^{\frac{s-1}{2}} n_j^{(i)} \equiv s \frac{q-1}{2} \equiv 0 \pmod{q-1},\end{aligned}$$

矛盾, 因此引理得证.

定理的证明

分三步来考虑:

* 1990 年 3 月 21 日.

(一) $A = 0$. 依定理所设 R 为一有限 Dedekind 整环, 故 R 为有限域, 从而 0 为一素理想, 依定理所设 $|R|$ 为奇数, 从而由引理知此时定理为真.

(二) $A = p_1^{e_1} \cdots p_k^{e_k}$ (诸 p_i 为互异素理想, 诸 $e_j > 0$), 至少有一 $e_i \geq 2$.

不妨设 $e_1 \geq 2$, 设 A 的完全剩余系中有 r 个属于 p_1 , 若有 A 的 s 不完全剩余系 $a_1^{(i)}, \dots, a_s^{(i)}$ ($1 \leq i \leq s$) 使 $\prod_{i=1}^r a_i^{(i)}, \dots, \prod_{i=1}^r a_s^{(i)}$ 也为 A 的完全剩余系, 则不妨设 $a_1^{(i)}, \dots, a_r^{(i)} \in p_1$, 而 $a_{r+1}^{(i)}, \dots, a_s^{(i)}$ 均不属于 p_1 ($1 \leq i \leq s$), 于是对任一 $x \in p_1$, 有 $x \equiv \prod_{i=1}^r a_i^{(i)} \pmod{A}$ ($1 \leq i \leq r$), 而 $s \geq 2, a_j^{(i)} \in p_1, e_1 \geq 2$, 故 $x \in p_1^2$. 故 $p_1 = p_1^2$, 与 R 为 Dedekind 整环矛盾. 故此时定理为真.

(三) $A = p_1 p_2 \cdots p_k$ (诸 p_i 为互异素理想), 此时依定理所设, 不妨令 R/p_i 为特征为奇数之域.

由中国剩余定理知, 可取诸 p_i 的完全剩余系

$$a_1^{(i)}, \dots, a_{N_i}^{(i)} \quad (1 \leq i \leq k, N_i | R/p_i |)$$

满足条件

$$a_1^{(i)} \equiv \cdots \equiv a_{N_i}^{(i)} \equiv x \pmod{p_j} \quad (j \neq i, \quad 1 \leq i \leq s, 1 \leq j \leq s),$$

其中 $x \in R - A$ 任意取定.

容易知道 $N_1 \cdots N_k$ 个积

$$a_1^{(1)}, \dots, a_{N_k}^{(k)} \quad (1 \leq i_1 \leq N_1, \dots, 1 \leq i_k \leq N_k) \quad (1)$$

构成 A 的完全剩余系. 而 $N_2 \cdots N_k$ 个积

$$a_2^{(2)} \cdots a_{N_k}^{(k)} \quad (2)$$

构成 $B = p_2 \cdots p_k$ 的完全剩余系. 设 $a = a_1^{(1)} \in p_1$, (2) 之一排列为 $\beta_1, \dots, \beta_{N_B}$ ($N_B = |R/B|$), 则 (2) 中属于 p_1 者恰为

$$a\beta_1, \dots, a\beta_{N_B} \quad (3)$$

因而若 A 的某 s 个完全剩余系 $a_1^{(i)}, \dots, a_s^{(i)}$ ($1 \leq i \leq s$) 使 $\prod_{i=1}^s a_i^{(i)}, \dots, \prod_{i=1}^s a_s^{(i)}$ 也为 A 的完全剩余系, 那就必得 (3) 的相应 s 个置换 $a\beta_1^{(i)}, \dots, a\beta_{N_B}^{(i)}$ ($1 \leq i \leq s$) 使 $a \prod_{i=1}^s \beta_1^{(i)}, \dots, a \prod_{i=1}^s \beta_{N_B}^{(i)}$ 也为 (3) 的置换, 但由 $a \equiv x \pmod{p_i}$ ($2 \leq i \leq k$), $x \in R - A$ 知, $\beta_1^{(i)}, \dots, \beta_{N_B}^{(i)}$ ($1 \leq i \leq s$) 及 $\prod_{i=1}^s \beta_1^{(i)}, \dots, \prod_{i=1}^s \beta_{N_B}^{(i)}$ 均为 β_1, \dots, N_{N_B} 的置换 (或 B 的完全剩余系). 同理可证, 对 $C = p_3 \cdots p_k$ 有同样结果, 如此下去可知, 对 p_k 也有同样结果. 但 R/p_k 为奇数阶有限域, 故有引理知矛盾. 至此, 定理证毕.

由于有理整数环 Z 及有限次代数数域的代数整数环均是 Dedekind 整环, 因而定理 A 和定理 B 都是本文定理的特例.

推论 R, A 及 s 同定理所设, 设 $f_i(x)$ ($1 \leq i \leq s$) 为 R/A 的置换多项式 (定义见 [4]), 则 $f(x) = \prod_{i=1}^s f_i(x)$ 不是 R/A 的置换多项式.

显见 [4] 中的定理 1.4 和定理 3.6 均为推论之特殊情形.

参考文献

- [1] Vijayaghavan, T., and Chowla, S., *On complete residue sets*, Quart. Math., Oxford Ser. 19(1948), 193—199.
- [2] Coles, W. J., and Olson, F. R., *A note on complete residue systems*, Amer. Math. Monthly., 61(1954), 622.
- [3] 孙琦, 旷京华, 关于代数数域中的完全剩余系, 数学学报, 2(1987), 226—228.
- [4] 孙琦, 万大庆, 置换多项式及其应用, 辽宁教育出版社, 沈阳, (1987).

On the Complete System of Residues in Dedekind Domain

Gao Weidong

(Dept. of Math., Northeast Normal University, Changchun, China)

Abstract

In this paper, we prove the following result: If R is a Dedekind domain, m is even and $m > 0$, A is an ideal of R such that

- (i) $|R/A|$ is a finite number,
 - (ii) $A \neq p_1 \cdots p_k$, p_1, \dots, p_k are distinct prime ideal of A and $|R/p_i|$ is even for every i ($1 \leq i \leq k$)
- then for any n 's complete system of residues of A , $a_1^{(i)}, \dots, a_N^{(i)}$ ($N = |R/A|$), $\prod_{i=1}^s a_1^{(i)}, \dots, \prod_{i=1}^s a_N^{(i)}$ is not a complete system of residues of A .