

# 模 $m$ 的 $k$ 次剩余个数

纪春岗

( 同济大学数学研究所 , 上海 200092 )

[ 摘要 ] 给出了模  $m$  的  $k$  次剩余个数的公式.

[ 关键词 ] 模  $m$  ;  $k$  次剩余 ; 同余方程

[ 中图分类号 ] O156 ; [ 文献标识码 ] A ; [ 文章编号 ] 1001-4616( 2001 ) 01-0001-02

## 0 引言

设  $m, k$  为正整数,  $i$  是一个整数. 若同余方程  $x^k \equiv i \pmod{m}$  有解, 则称  $i$  为模  $m$  的  $k$  次剩余. 否则称  $i$  为模  $m$  的  $k$  次非剩余. 对于奇素数  $p$ , 熟知模  $p$  的二次剩余与二次非剩余的个数分别是  $(p+1)/2$  和  $(p-1)/2$ . 本文给出了模  $m$  的  $k$  次剩余个数的公式, 具体地说, 令  $S_k(m) = \#\{i \mid x^k \equiv i \pmod{m} \text{ 有解且 } 0 \leq i \leq m-1\}$ . 本文给出了  $S_k(m)$  的公式. 显然  $S_1(m) = m$ . 本文以下均设  $k \geq 2, m = 2^\beta p_1^{\alpha_1} p_2^{\alpha_2} \dots p_s^{\alpha_s}$ , 其中  $p_1, p_2, \dots, p_s$  为互不相同的奇素数.

## 1 主要定理

定理 1  $S_k(m) = S_k(2^\beta) S_k(p_1^{\alpha_1}) \dots S_k(p_s^{\alpha_s})$ .

定理 2 设  $p$  为一个奇素数,  $\alpha$  是一个正整数,  $k \geq 1$ , 则

$$S_k(p^\alpha) = 1 + \frac{(p-1)p^{\alpha-1}}{(k, p-1)} \sum_{\substack{0 \leq j \leq (\alpha-1)/k \\ j \in \mathbf{Z}}} \frac{1}{(p^{jk} k, p^{\alpha-1})},$$

其中  $(*, *)$  表示最大公约数.

定理 3 (1)  $S_k(2) = 2, k \geq 2$ ;

$$(2) k \geq 2, \beta \geq 2 \text{ 时, 有 } S_k(2^\beta) = \lambda(k, \beta) + 1 + \frac{2^{\beta-1}}{(k, 2)} \sum_{\substack{0 \leq j \leq (\beta-2)/k \\ j \in \mathbf{Z}}} \frac{1}{(2^{jk} k, 2^{\beta-2})}, \text{ 其中 } \lambda(k, \beta) = \begin{cases} 1, & \text{如果 } \beta \equiv 1 \pmod{k}; \\ 0, & \text{否则.} \end{cases}$$

$$\text{推论 4 } S_k(m) = (2 + \frac{1}{3}(2^{\beta-1} - 2^{1+(-1)^{\beta/2}})) \prod_{1 \leq j \leq s} (1 + \frac{1}{2(p_j+1)} \{ p_j^{\alpha_j+1} - p_j^{(1+(-1)^{\alpha_j/2})} \}).$$

## 2 几个引理

引理 1 设  $p$  为一个素数,  $k, \alpha$  为正整数,  $1 \leq i = p^j i' < p^\alpha$  且  $(i', p) = 1$ , 则同余方程  $x^k \equiv$

$i(\bmod p^\alpha)$  有解的充分必要条件是  $k \mid j$  且  $x^k \equiv i'(\bmod p^{\alpha-j})$  也有解.

设  $p$  为一个素数, 令  $S_k^*(p^\alpha) = \#\{i \mid x^k \equiv i(\bmod p^\alpha) (i, p) = 1 \text{ 且 } 1 \leq i < p^\alpha\}$ .

引理 2 若  $p$  为一个奇素数且  $\alpha, k$  均为正整数, 则  $S_k^*(p^\alpha) = \frac{(p-1)p^{\alpha-1}}{(k, p-1)p^{\alpha-1}}$ .

证明 因为模  $p^\alpha$  存在原根, 不妨设  $g$  为它的一个原根, 则同余方程  $x^k \equiv i(\bmod p^\alpha) (i, p) = 1$  有解等价于同余方程  $k \operatorname{ind}_g x \equiv \operatorname{ind}_g i(\bmod \phi(p^\alpha))$  有解, 而后一个同余方程有解当且仅当  $(k, \phi(p^\alpha)) \mid \operatorname{ind}_g i$ . 又因为  $0 \leq \operatorname{ind}_g i < \phi(p^\alpha)$ , 从而

$$S_k^*(p^\alpha) = \frac{(p-1)p^{\alpha-1}}{(k, p-1)p^{\alpha-1}}.$$

引理 3 设  $\beta, k$  均为正整数且  $\beta \geq 2$ , 则  $S_k^*(2^\beta) = \frac{2}{(k, 2)} \frac{2^{\beta-2}}{(k, 2^{\beta-2})}$ .

证明  $\beta = 2$  时, 模 4 有原根存在, 与引理 2 的证明类似可得  $S_k^*(4) = \frac{2}{(k, 2)}$ . 当  $\beta \geq 3$  时,

由文 [1] 可知, 任一奇数  $i, 1 \leq i < 2^\beta$ , 存在唯一的  $b (0 \leq b < 2^{\beta-2})$ , 使得  $i \equiv (-1)^{\frac{i-1}{2}} 5^b (\bmod 2^\beta)$ .

因此  $x^k \equiv i(\bmod 2^\beta)$  有解当且仅当同余方程组  $\begin{cases} ky \equiv \frac{i-1}{2} (\bmod 2) \\ kz \equiv b (\bmod 2^{\beta-2}) \end{cases}$  有解. 因此

$$S_k^*(2^\beta) = \frac{2}{(k, 2)} \frac{2^{\beta-2}}{(k, 2^{\beta-2})}.$$

### 3 定理的证明

定理 1 的证明 利用同余方程的性质以及孙子定理即可.

定理 2 的证明 利用引理 1 和引理 2 得

$$\begin{aligned} S_k(p^\alpha) &= 1 + \sum_{\substack{0 \leq j \leq \frac{\alpha-1}{k} \\ j \in \mathbb{Z}}} S_k^*(p^{\alpha-kj}) = 1 + \sum_{\substack{0 \leq j \leq \frac{\alpha-1}{k} \\ j \in \mathbb{Z}}} \frac{(p-1)p^{\alpha-kj-1}}{(k, p-1)p^{\alpha-kj-1}} \\ &= 1 + \frac{(p-1)p^{\alpha-1}}{(k, p-1)} \sum_{\substack{0 \leq j \leq \frac{\alpha-1}{k} \\ j \in \mathbb{Z}}} \frac{1}{(p^j k, p^{\alpha-1})}. \end{aligned}$$

定理 3 的证明 利用引理 1 和引理 3, 证明类似于定理 2.

### [参考文献]

- [1] 华罗庚. 数论导引[M]. 北京: 科学出版社, 1979.

## The Number of $k$ th Power Residues Modulo $m$

Ji Chungang

(Institute of Mathematics, Tongji University, Shanghai 200092, PRC)

**Abstract** In this paper, the author give a formula of the number of  $k$ th power residues modulo  $m$ .

**Key words** modulo  $m$ ;  $k$ th power residue; congruence equation

[责任编辑 陆炳新]