# 3 指标及$n$次剩余

在$m = p^\alpha$ 或$2p^\alpha$ 的情形下, 模$m$ 的原根$g$ 是存在的. 利用原根引进指标概念, 并研究

$$x^n \equiv a \pmod m, \quad (a, m) = 1$$

有解的条件及解数.

对任意的整数$a$, $(a, m) = 1$, 存在惟一的整数$r$, $1 \le r \le \varphi(m)$, 使得

$$g^r \equiv a \pmod m.$$

**定义1** 设$m$ 是大于1 的整数, $g$ 是模$m$ 的一个原根. 设$a$ 是一个与$m$互素的整数. 则存在惟一的整数$r$ 使得

$$g^r \equiv a \pmod m, \quad 1 \le r \le \varphi(m)$$

成立, 这个整数$r$ 叫做以$g$ 为底的$a$ 对模$m$ 的一个指标, 记作$r = \mathrm{ind}_g a$ (或$r = \mathrm{ind} a$).

**例1** 整数5 是模17 的原根. 并且我们有

| $5^1$ | $5^2$ | $5^3$ | $5^4$ | $5^5$ | $5^6$ | $5^7$ | $5^8$ | $5^9$ | $5^{10}$ | $5^{11}$ | $5^{12}$ | $5^{13}$ | $5^{14}$ | $5^{15}$ | $5^{16}$ |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 5 | 8 | 6 | 13 | 14 | 2 | 10 | -1 | 12 | 9 | 11 | 4 | 3 | 15 | 7 | 1 |

因此, 我们有

$$\begin{array}{llll}
\mathrm{ind}_5 1 = 16, & \mathrm{ind}_5 2 = 6, & \mathrm{ind}_5 3 = 13, & \mathrm{ind}_5 4 = 12, \\
\mathrm{ind}_5 5 = 14, & \mathrm{ind}_5 6 = 3, & \mathrm{ind}_5 7 = 15, & \mathrm{ind}_5 8 = 2, \\
\mathrm{ind}_5 9 = 10, & \mathrm{ind}_5 10 = 7, & \mathrm{ind}_5 11 = 11, & \mathrm{ind}_5 12 = 9, \\
\mathrm{ind}_5 13 = 4, & \mathrm{ind}_5 14 = 5, & \mathrm{ind}_5 15 = 14, & \mathrm{ind}_5 16 = 8.
\end{array}$$

**定理2** 设$g$ 是原根. 设$(a,m)=1$. 如果$r$ 使得

$$g^r \equiv a \pmod{m}$$

成立, 则这个整数$r$ 满足$r \equiv \mathrm{ind}_g a \pmod{\varphi(m)}$.

**证** 因为$(a,m)=1$, 所以

$$g^r \equiv a \equiv g^{\mathrm{ind}_g a} \pmod{m}.$$

从而, $g^{r-\mathrm{ind}_g a} \equiv 1 \pmod{m}$.

又因为$g$ 模$m$ 的指数是$\varphi(m)$, $\varphi(m) \mid r-\mathrm{ind}_g a$. 因此,

$$r \equiv \mathrm{ind}_g a \pmod{\varphi(m)}.$$

**推论** 设$g$ 是原根. 设$(a,m)=1$. 则

$$\mathrm{ind}_g 1 \equiv 0 \pmod{\varphi(m)}.$$

**证** 因为$g^0 \equiv 1 \pmod{m}$, 根据定理2, 我们有

$$\mathrm{ind}_g 1 \equiv 0 \pmod{\varphi(m)}.$$

**定理3** 设$m$ 是大于$1$ 的整数, $g$ 是模$m$ 的一个原根, $r$ 是一个整数, 满足$1 \le r \le \varphi(m)$. 则以$g$ 为底的对模$m$ 有相同指标$r$ 的所有整数全体是模$m$ 的一个简化剩余类.

**证** 显然, 我们有

$$\mathrm{ind}_g g^r = r, \quad (g^r, m) = 1.$$

根据指标的定义, 整数$a$ 的指标$\mathrm{ind}_g a = r$ 的充分必要条件是

$$a \equiv g^r \pmod{m}.$$

故以$g$ 为底对模$m$ 有同一指标$r$ 的所有整数都属于$g^r$ 所在的模$m$ 的一个简化剩余类.

**定理4** 设$m$ 是大于1 的整数, $g$ 是模$m$ 的一个原根. 若$a_1, \ldots, a_n$ 是与$m$ 互素的$n$ 个整数, 则

$$\mathrm{ind}_g(a_1 \cdots a_n) \equiv \mathrm{ind}_g(a_1) + \cdots + \mathrm{ind}_g(a_n) \pmod{\varphi(m)}.$$

特别地, $\mathrm{ind}_g(a^n) \equiv n\,\mathrm{ind}_g(a) \pmod{\varphi(m)}$.

**证** 令$r_i = \mathrm{ind}_g(a_i),\ i = 1, \ldots, n$. 根据指标的定义, 我们有

$$a_i \equiv g^{r_i} \pmod{m}, \quad i = 1, \ldots, n.$$

从而$a_1 \cdots a_r \equiv g^{r_1+\cdots+r_n} \pmod{m}$.

根据定理1, 我们得到

$$\mathrm{ind}_g(a_1 \cdots a_n) \equiv \mathrm{ind}_g(a_1) + \cdots + \mathrm{ind}_g(a_n) \pmod{\varphi(m)}.$$

特别地, 对于$a_1 = \cdots = a_n = a$, 有

$$\mathrm{ind}_g(a^n) \equiv n\,\mathrm{ind}_g(a) \pmod{\varphi(m)}.$$

**例2** 作模41 的指标表.

**解** 已知6 是模41 的原根, 直接计算$g^r \pmod m$:

$$
\begin{array}{lllllll}
6^{40} \equiv 1, & 6^1 \equiv 6, & 6^2 \equiv 19, & 6^3 \equiv 11, & 6^4 \equiv 25, & 6^5 \equiv 27, & 6^6 \equiv 39, \\
6^8 \equiv 10, & 6^9 \equiv 19, & 6^{10} \equiv 32, & 6^{11} \equiv 28, & 6^{12} \equiv 4, & 6^{13} \equiv 24, & 6^{14} \equiv 21, \\
6^{16} \equiv 18, & 6^{17} \equiv 26, & 6^{18} \equiv 33, & 6^{19} \equiv 34, & 6^{20} \equiv 40, & 6^{21} \equiv 35, & 6^{22} \equiv 5, \\
6^{24} \equiv 16, & 6^{25} \equiv 14, & 6^{26} \equiv 2, & 6^{27} \equiv 12, & 6^{28} \equiv 31, & 6^{29} \equiv 22, & 6^{30} \equiv 9, \\
6^{32} \equiv 37, & 6^{33} \equiv 17, & 6^{34} \equiv 20, & 6^{35} \equiv 38, & 6^{36} \equiv 23, & 6^{37} \equiv 15, & 6^{38} \equiv 8,
\end{array}
$$

**数的指标**: 第一列表示十位数, 第一行表示个位数,交叉位置表示指标所对应数.

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | | 40 | 26 | 15 | 12 | 22 | 1 | 39 | 38 | 30 |
| 1 | 8 | 3 | 27 | 31 | 25 | 37 | 24 | 33 | 16 | 9 |
| 2 | 34 | 14 | 29 | 36 | 13 | 4 | 17 | 5 | 11 | 7 |
| 3 | 23 | 28 | 10 | 18 | 19 | 21 | 2 | 32 | 35 | 6 |
| 4 | 20 | | | | | | | | | |

| | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | | 40 | 26 | 15 | 12 | 22 | 1 | 39 | 38 | 30 |
| 1 | 8 | 3 | 27 | 31 | 25 | 37 | 24 | 33 | 16 | 9 |
| 2 | 34 | 14 | 29 | 36 | 13 | 4 | 17 | 5 | 11 | 7 |
| 3 | 23 | 28 | 10 | 18 | 19 | 21 | 2 | 32 | 35 | 6 |
| 4 | 20 | | | | | | | | | |

**例3** 分别求整数$a = 28, 18$ 以6 为底模41 的指标.

**解** 根据模41的以原根$g = 6$ 的指数表, 查找十位数2 所在行, 个位数8 所在列, 交叉位置的数11 就是$\mathrm{ind}_6 28 = 11$. 而查找十位数1 所在行, 个位数8 所在列, 交叉位置的数16 就是$\mathrm{ind}_6 18 = 16$.

为什么要列表呢? 这是因为从整数$r$ 计算

$$g^r \equiv a \pmod m$$

很容易; 但从整数$a$ 求整数$r$ 使得

$$g^r \equiv a \pmod m$$

就非常困难.

**定义2** 设$m$ 是大于1 的整数, $a$ 是与$m$ 互素的整数. 如果$n$ 次同余式

$$x^n \equiv a \pmod m \qquad (1)$$

有解, 则$a$ 叫做对模$m$ 的$n$ **次剩余**; 否则, $a$ 叫做对模$m$ 的$n$ **次非剩余**.

**例4** 求5 次同余式$x^5 \equiv 9 \pmod{41}$的解.

**解** 从模41 的指标表, 查找整数9 的十位数0 所在的行, 个位数9 所在的列, 交叉位置的数30 就是$\mathrm{ind}_6 9 = 30$. 再令$x = 6^y \pmod{41}$. 原同余式就变为

$$6^{5y} \equiv 6^{30} \pmod{41}.$$

因为6 是模41 的原根, 根据定理2 我们有

$$5y \equiv 30 \pmod{40} \quad \text{或} \quad y \equiv 6 \pmod{8}.$$

解得$y \equiv 6,\ 14,\ 22,\ 30,\ 38 \pmod{40}$. 因此, 原同余式的解为

$$\begin{aligned} &x \equiv 6^6 \equiv 39,\ x \equiv 6^{14} \equiv 21,\ x \equiv 6^{22} \equiv 5,\\ &x \equiv 6^{30} \equiv 9,\ x \equiv 6^{38} \equiv 8,\ \ x \equiv 6^{39} \equiv 7 \pmod{41}. \end{aligned}$$

**定理5** 设$g$ 是原根. 设$(a,m)=1$ . 则

$$x^n \equiv a \pmod m \tag{2}$$

有解的充分必要条件是

$$(n,\varphi(m)) \mid \mathrm{ind}a,$$

且在有解的情况下, 解数为$(n,\varphi(m))$.

**证** 若同余式(2)有解$x \equiv x_0 \pmod m$,

则分别存在非负整数$u$, $r$ 使得$x_0 \equiv g^u, \quad a \equiv g^r \pmod m$.

由(2)得$g^{un} \equiv g^r \pmod m$ 或$un \equiv r \pmod{\varphi(m)}$.

即同余式 $nX \equiv r \pmod{\varphi(m)}$ (3) 有解$X \equiv u \pmod{\varphi(m)}$. 因此, $(n,\varphi(m)) \mid \mathrm{ind}a$.

反过来, 若$(n,\varphi(m)) \mid \mathrm{ind}a$, 则(3)有解$X \equiv u \pmod{\varphi(m)}$, 且解数为$(n,\varphi(m))$. 因此, (2)有解$x_0 \equiv g^u \pmod m$, 解数为$(n,\varphi(m))$.

**推论** 在定理5的假设条件下, $a$ 是模$m$ 的$n$ 次剩余的充分必要条件是

$$a^{\varphi(m)/d} \equiv 1 \pmod{m}, \quad d = (n, \varphi(m)).$$

**证** 由定理5之证明: 同余式

$$x^n \equiv a \pmod{m}$$

有解的充分必要条件是同余式

$$nX \equiv r \pmod{\varphi(m)}$$

有解. 而这等价于

$$(n, \varphi(m)) \mid \mathrm{ind} a,$$

即$\mathrm{ind} a \equiv 0 \pmod{d}$.

两端同乘$\dfrac{\varphi(m)}{d}$, 得到$\frac{\varphi(m)}{d}\mathrm{ind} a \equiv 0 \pmod{\varphi(m)}$.

这等价于$a^{\varphi(m)/d} \equiv 1 \pmod{m}$.

**例5** 求解同余式$x^8 \equiv 23 \pmod{41}$.

**解** 因为

$$d=(n,\varphi(m))=(8,\varphi(41))=(8,40)=8, \quad \mathrm{ind}23=36.$$

又36 不能被8 整除, 所以同余式无解.

**例6** 求解同余式$x^{12} \equiv 37 \pmod{41}$.

**解** 因为

$$d = (n, \varphi(m)) = (12, \varphi(41)) = (12, 40) = 4,$$
$$\mathrm{ind}37 = 32.$$

又$4|32$, 所以同余式有解. 现求解等价的同余式:

$$12\ \mathrm{ind}x \equiv \mathrm{ind}37 \pmod{40}$$

或$3\ \mathrm{ind}x \equiv 8 \pmod{10}$.

得到$\mathrm{ind}x \equiv 6,\ 16,\ 26,\ 36 \pmod{40}$.

查指标表得原同余式解

$$x \equiv 39,\ 18,\ 2,\ 23 \pmod{41}.$$

**定理6** 设$g$ 是原根, $(a, m) = 1$ . 则$a$ 对模$m$ 的指数是

$$e = \frac{\varphi(m)}{(\mathrm{ind}a, \varphi(m))}.$$

特别地, $a$ 是模$m$ 的原根当且仅当$(\mathrm{ind}a, \varphi(m)) = 1.$

**证** 因为模$m$ 有原根$g$, 所以有

$$a = g^{\mathrm{ind}a} \pmod{m}.$$

根据§5.1 定理3, $a$ 的指数为

$$\mathrm{ord}(a) = \mathrm{ord}(g^{\mathrm{ind}a}) = \frac{\mathrm{ord}(g)}{(\mathrm{ord}(g), \mathrm{ind}a)} = \frac{\varphi(m)}{(\mathrm{ind}a, \varphi(m))}.$$

显然, $a$ 是模$m$ 的原根的充分必要条件是

$$\mathrm{ord}(a) = \varphi(m),$$

即

$$(\mathrm{ind}a, \varphi(m)) = 1.$$

**定理7** 设$g$ 是模$m$ 的一个原根. 则模$m$ 的简化剩余系中, 指数是$e$ 的整数个数是$\varphi(e)$. 特别地, 在模$m$ 的简化剩余系中, 原根的个数是$\varphi(\varphi(m))$.

**证** 因为模$m$ 有原根$g$, 根据§5.1 定理3, 知$a = g^d$ 的指数为

$$\operatorname{ord}(a) = \operatorname{ord}(g^d) = \frac{\operatorname{ord}(g)}{(\operatorname{ord}(g), d)} = \frac{\varphi(m)}{(d, \varphi(m))}.$$

显然, $a$ 的指数是$e$ 的充分必要条件是$\dfrac{\varphi(m)}{(d, \varphi(m))} = e$, 即

$$(d, \varphi(m)) = \frac{\varphi(m)}{e}.$$

令$d = d'\dfrac{\varphi(m)}{e}, \quad 0 \le d' < e$. 上式等价于$(d', e) = 1$. 易知这样的$d'$ 有$\varphi(e)$ 个. 从而指数为$\varphi(m)$ 的整数个数是$\varphi(\varphi(m))$. 即原根个数是$\varphi(\varphi(m))$.