第七章　原 根

原根是数论的理论和应用中一个很重要的概念。本章要介绍原根以及与它有关的基本知识。

第一节　指数及其基本性质

定义 1　设 $m > 1$，$(a, m) = 1$，则使

$$a^r \equiv 1 \pmod{m} \tag{1}$$

成立的最小的正整数r，称为a对模m的指数，记为$\delta_m(a)$，在不致误会的情况下，简记为$\delta(a)$。

由Euler定理，当$r = \varphi(m)$时式(1)成立，因此，恒有$\delta_m(a) \le \varphi(m)$。

若$a \equiv b \pmod{m}$，$(a, m) = 1$，则显然有$\delta_m(a) = \delta_m(b)$。

定义 2　若$\delta_m(a) = \varphi(m)$，则称a是模m的原根。

例如，当 $m = 7$ 时，因为

$$2^1 \equiv 2，2^2 \equiv 4，2^3 \equiv 1 \pmod{7}，$$

所以$\delta_7(2) = 3$。又因为

$$3^1 \equiv 3，3^2 \equiv 2，3^3 \equiv 6，3^4 \equiv 4，3^5 \equiv 5，3^6 \equiv 1 \pmod{7}，$$

所以$\delta_7(3) = 6 = \varphi(7)$，3 是模 7 的原根。

以后，在谈到 a 对模 m 的指数时，总假定 $m > 1$，$(a, m) = 1$。

定理 1　记$\delta = \delta_m(a)$，则

$$a^0, a^1, \cdots, a^{\delta - 1}$$

对模 m 两两不同余。

证明　用反证法。若有 $0 \le i < j \le \delta - 1$，使得

$$a^i \equiv a^j \pmod{m}，$$

则由$(a, m) = 1$ 得到

$$a^{j-i} \equiv 1 \pmod{m}，$$

这与$\delta = \delta_m(a)$的定义矛盾，所以定理成立。证毕。

定理 1 说明，若 g 是模 m 的原根，则

$$g^0, g^1, \cdots, g^{\varphi(m)-1}$$

构成模 m 的简化剩余系。

定理 2　设$\delta = \delta_m(a)$，r与r'是正整数，则

$$a^r \equiv a^{r'} \pmod m \tag{2}$$

的充要条件是

$$r \equiv r' \pmod \delta。\tag{3}$$

特别地，$a^r \equiv 1 \pmod m$的充要条件是$\delta \mid r$。

证明　不妨设 $r > r'$。因为$(a, m) = 1$，所以式(2)等价于

$$a^{r-r'} \equiv 1 \pmod m。\tag{4}$$

若式(4)成立，记$r - r' = q\delta + t$，$q \in \mathbf{N}$，$0 \le t < \delta$，则由定义 1，有

$$a^t \equiv a^{q\delta+t} = a^{r-r'} \equiv 1 \pmod m。$$

由$\delta_m(a)$的定义可知$t = 0$，即$\delta \mid r - r'$，也即式(3)成立。必要性得证。

若式(3)成立，则存在$q \in \mathbf{N}$，使得$r - r' = q\delta$，则由定义 1，有

$$a^{r-r'} = a^{q\delta} \equiv 1 \pmod m，$$

即式(4)成立，从而式(2)成立，充分性得证。

取$r' = 0$，得到定理的第二个结论。证毕。

推论　$\delta_m(a) \mid \varphi(m)$。

证明　由 Euler 定理及定理 2 得证。

定理 3　设 k 是非负整数，则

$$\delta_m(a^k) = \frac{\delta_m(a)}{(\delta_m(a), k)}。$$

证明　记$\delta = \delta_m(a)$，$\delta' = \delta_m(a^k)$，$\delta'' = \dfrac{\delta}{(\delta, k)}$，则由定理 2 及

$$a^{k\delta''} \equiv 1 \pmod m$$

可知

$$\delta' \mid \delta''。\tag{5}$$

由定理 2 及$a^{k\delta'} = (a^k)^{\delta'} \equiv 1 \pmod m$可知$\delta \mid k\delta'$，因此

$$\delta'' = \frac{\delta}{(\delta, k)} \,\Big|\, \frac{k\delta'}{(\delta, k)}。\tag{6}$$

由于$\left(\dfrac{\delta}{(\delta, k)}, \dfrac{k}{(\delta, k)}\right) = 1$，所以由式(6)可以推出$\delta'' \mid \delta'$。由此及式(5)得

到$\delta'' = \delta'$。证毕。

推论 若$\delta_m(a) = kl$，$k > 0$，$l > 0$，则$\delta_m(a^k) = l$。

定理 4 等式

$$\delta_m(ab) = \delta_m(a)\delta_m(b) \tag{7}$$

与

$$(\delta_m(a), \delta_m(b)) = 1 \tag{8}$$

是等价的。

证明 记$\delta_1 = \delta_m(a)$，$\delta_2 = \delta_m(b)$，$\delta_3 = \delta_m(ab)$，$\lambda = [\delta_1, \delta_2]$。

若式(7)成立，则$\lambda \mid \delta_1\delta_2 = \delta_3$。由$\lambda$的定义和定理 2，以及

$$(ab)^{\lambda} = a^{\lambda}b^{\lambda} \equiv 1 \pmod m$$

又得到$\delta_3 \mid \lambda$。因此$\delta_3 = \lambda$，即$\delta_1\delta_2 = [\delta_1, \delta_2]$，所以$(\delta_1, \delta_2) = 1$，即式(8)成立。

若式(8)成立，则由定理 2 及

$$1 \equiv [(ab)^{\delta_3}]^{\delta_2} \equiv (ab)^{\delta_3\delta_2} \equiv a^{\delta_3\delta_2} \pmod m$$

得到$\delta_1 \mid \delta_2\delta_3$。由式(8)推出$\delta_1 \mid \delta_3$。同理可推出$\delta_2 \mid \delta_3$。所以

$$\lambda = [\delta_1, \delta_2] \mid \delta_3。$$

但是，由式(8)可知$[\delta_1, \delta_2] = \delta_1\delta_2$，所以

$$\delta_1\delta_2 \mid \delta_3。$$

另一方面，由定理 2 及

$$(ab)^{\delta_1\delta_2} \equiv 1 \pmod m$$

得到$\delta_3 \mid \delta_1\delta_2$。所以$\delta_3 = \delta_1\delta_2$，即式(7)成立。证毕。

例 1 求 1，2，3，4，5，6 对模 7 的指数。

根据定义 1 直接计算，得到

$$\delta_7(1) = 1，\delta_7(2) = 3，\delta_7(3) = 6，$$
$$\delta_7(4) = 3，\delta_7(5) = 6，\delta_7(6) = 2。$$

例 1 中的结果可列表如下：

a	1	2	3	4	5	6
$\delta_7(a)$	1	3	6	3	6	2

这样的表称为指数表。这个表就是模 7 的指数表。

下面是模 10 的指数表：

a	1	3	7	9
$\delta_{10}(a)$	1	4	4	2

例 2　若$(a, m) = 1$，$aa' \equiv 1 \pmod m$，则

$$\delta_m(a) = \delta_m(a')。$$

解　显然$(a', m) = 1$。要证明的结论由

$$a^d \equiv 1 \pmod m \Longleftrightarrow (a')^d \equiv 1 \pmod m$$

即可得出。

例 3　若$n \mid m$，则$\delta_n(a) \mid \delta_m(a)$。

解　由 $n \mid m$ 及定理 2 有

$$a^{\delta_m(a)} \equiv 1 \pmod m \Longrightarrow a^{\delta_m(a)} \equiv 1 \pmod n \Longrightarrow \delta_n(a) \mid \delta_m(a)。$$

例 4　若$(m, n) = 1$，$(a, mn) = 1$，则

$$\delta_{mn}(a) = [\delta_m(a), \delta_n(a)]。\tag{9}$$

解　记$\delta = \delta_{mn}(a)$，$\delta' = [\delta_m(a), \delta_n(a)]$，由例 3 有

$$\delta_m(a) \mid \delta,\quad \delta_n(a) \mid \delta \Longrightarrow \delta' \mid \delta。\tag{10}$$

又由

$$a^{\delta'} \equiv 1 \pmod m，\quad a^{\delta'} \equiv 1 \pmod n$$

得到

$$a^{\delta'} \equiv 1 \pmod{mn}。$$

因此，由定理 2，有$\delta \mid \delta'$。由此及式(10)推出式(9)。

例 5　若$(m, n) = 1$，a_1，a_2是任意整数，$(a_1, m) = (a_2, n) = 1$，则存在整数a，$(a, mn) = 1$，使得

$$\delta_{mn}(a) = [\delta_m(a_1), \delta_n(a_2)]。$$

解　设方程组

$$\begin{cases} x \equiv a_1 \pmod m \\ x \equiv a_2 \pmod n \end{cases}$$

的解是 $x \equiv a \pmod{mn}$，则$(a, mn) = 1$，并且由例 4 可知

$$\delta_{mn}(a) = [\delta_m(a), \delta_n(a)] = [\delta_m(a_1), \delta_n(a_2)]。$$

习　题　一

1.　写出模 11 的指数表。

2. 求模 14 的全部原根。

3. 设 $m > 1$，模 m 有原根，d 是 $\varphi(m)$ 的任一个正因数，证明：在模 m 的简化剩余系中，恰有 $\varphi(d)$ 个指数为 d 的整数，并由此推出模 m 的简化剩余系中恰有 $\varphi(\varphi(m))$ 个原根。

4. 设 $m \ge 3$，g 是模 m 的原根，$x_1, x_2, \cdots, x_{\varphi(m)}$ 是模 m 的简化剩余系，证明：

(ⅰ) $g^{\frac{\varphi(m)}{2}} \equiv -1 \pmod{m}$；

(ⅱ) $x_1 x_2 \cdots x_{\varphi(m)} \equiv -1 \pmod{m}$。

5. 设 $p = 2^n + 1$ 是一个奇素数，证明：模 p 的全部二次非剩余就是模 p 的全部原根。

6. 证明：

(ⅰ) 设 p 奇素数，则 $M_p = 2^p - 1$ 的素因数必为 $2pk + 1$ 型；

(ⅱ) 设 $n \ge 0$，则 $F_n = 2^{2^n} + 1$ 的素因数必为 $2^{n+1}k + 1$ 型。

第二节　原 根

对于什么样的正整数 m，模 m 的原根是存在的？这是本节要研究的问题。

为了叙述方便，对于正整数 n，设它的标准分解式是

$$n = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

其中 p_i（$1 \le i \le k$）是奇素数，记

$$\lambda(n) = [\varphi(2^{\alpha}), \varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}), \cdots, \varphi(p_k^{\alpha_k})]。$$

定理 1　模 m 有原根的必要条件是 $m = 1$，2，4，p^{α} 或 $2p^{\alpha}$，其中 p 是奇素数，$\alpha \ge 1$。

证明　若 m 不具备定理中所述形式，则必是

$$m = 2^{\alpha}\text{（}\alpha \ge 3\text{），} \tag{1}$$

$$m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\ \text{（}\alpha \ge 2\text{，}k \ge 1\text{），} \tag{2}$$

或

$$m = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}\ \text{（}\alpha \ge 0\text{，}k \ge 2\text{），} \tag{3}$$

其中p_i（$1 \le i \le k$）是奇素数，α_i（$1 \le i \le k$）是正整数。

如果 m 是形如式(2)的数，那么对于任意的 a，$(a, m) = 1$，有

$$a^{\varphi(2^\alpha)} \equiv 1 (\bmod 2^\alpha),$$

$$a^{\varphi(p_i^{\alpha_i})} \equiv 1 (\bmod p_i^{\alpha_i}), \quad 1 \le i \le k,$$

$$a^{\lambda(m)} \equiv 1 (\bmod 2^\alpha),$$

$$a^{\lambda(m)} \equiv 1 (\bmod p_i^{\alpha_i}), \quad 1 \le i \le k,$$

$$a^{\lambda(m)} \equiv 1 \ (\bmod m)。 \tag{4}$$

容易验证

$$\lambda(m) < \varphi(m)。$$

因此，由式(4)可知，任何与 m 互素的数 a 不是模 m 的原根。

同样方法可以证明，若 m 是形如式(1)或式(3)中的数，模 m 也没有原根。证毕。

下面我们要证明，定理 1 中的条件也是充分条件。为此，先要证明几个引理。

引理 1 设 m 是正整数。对任意的整数 a，b，一定存在整数 c，使得

$$\delta_m(c) = [\delta_m(a), \delta_m(b)]。$$

证明 由第一章第六节习题 6，存在正整数λ_1，λ_2，μ_1，μ_2，使得

$$\delta_m(a) = \lambda_1\lambda_2，\ \delta_m(b) = \mu_1\mu_2，\ (\lambda_2, \mu_2) = 1,$$

$$[\delta_m(a), \delta_m(b)] = \lambda_2\mu_2。 \tag{5}$$

由第一节定理 3，有

$$\delta_m(a^{\lambda_1}) = \lambda_2, \quad \delta_m(b^{\mu_1}) = \mu_2,$$

因此，由第一节定理 4 得到

$$\delta_m(a^{\lambda_1}b^{\mu_1}) = \delta_m(a^{\lambda_1})\delta_m(b^{\mu_1}) = \lambda_2\mu_2 = [\delta_m(a), \delta_m(b)]。$$

取 $c = a^{\lambda_1}b^{\mu_1}$ 即可得证。证毕。

引理 2 若 p 是奇素数，则模 p 有原根。

证明 由引理 1 及归纳法容易证明，存在整数 g，$(g, p) = 1$，使得

$$\delta = \delta_p(g) = [\delta_p(1), \delta_p(2), \cdots, \delta_p(p-1)]。$$

显然

$$\delta \mid p-1，\ \delta_p(j) \mid \delta，\ 1 \le j \le p-1。 \tag{6}$$

另一方面，由式（6）可知同余方程

$$x^{\delta}-1\equiv 0 \pmod p$$

有解 $x\equiv i \pmod p$，$1\le i\le p-1$。所以，由第五章第四节定理 2，可知，$p-1\le\delta$。由此及式(6)，得到 $p-1=\delta$，即 g 是模 p 的原根。证毕。

引理 3 设p是奇素数，α是正整数，则模p^{α}有原根。

证明 不妨设$\alpha>1$。设g是模p的原根，则$(g, p)=1$。因此，存在整数x_0，使得

$$g^{p-1}=1+px_0\ ,$$

因此，对于任意的整数 t，有

$$(g+pt)^{p-1}=g^{p-1}+p(p-1)tg^{p-2}+\cdots=1+p(x_0-g^{p-2}t)+p^2Q_2,$$

其中$Q_2\in\mathbf{Z}$，即

$$(g+pt)^{p-1}\equiv 1+p(x_0-g^{p-2}t) \pmod{p^2}。\tag{7}$$

取

$$t_0=0,\quad 当p\nmid x_0;$$
$$t_0=1,\quad 当p\mid x_0,$$

则$p\nmid x_0-g^{p-2}t_0=y_0$，于是

$$(g+pt_0)^{p-1}=1+py_0\not\equiv 1 \pmod{p^2},\ p\nmid y_0。\tag{8}$$

由式(8)，有

$$(g+pt_0)^{p(p-1)}=(1+py_0)^p=1+p^2y_1,$$

其中

$$y_1=y_0+\mathrm{C}_p^2y_0{}^2+\cdots+p^{p-2}y_0{}^p\equiv y_0 \pmod p。\tag{9}$$

因此，$p\nmid y_1$。类似地，由式(9)可以依次得到

$$\begin{aligned}
&(g+pt_0)^{p^2(p-1)}=(1+p^2y_1)^p=1+p^3y_2,\\
&(g+pt_0)^{p^3(p-1)}=(1+p^3y_1)^p=1+p^4y_3,\\
&\qquad\cdots\cdots\\
&(g+pt_0)^{p^{\alpha-1}(p-1)}=(1+p^{\alpha-1}y_1)^p=1+p^{\alpha}y_{\alpha-1},
\end{aligned}\tag{10}$$

其中$y_{\alpha-1}\equiv y_{\alpha-2}\equiv\cdots\equiv y_0 \pmod p$。因此

$$p\nmid y_i,\ 0\le i\le\alpha-1。\tag{11}$$

由于g是模p的原根，所以$g+pt_0$也是模p的原根，设$g+pt_0$对模p^{α}的指数是δ，则有

$$(g + pt_0)^{\delta} \equiv 1 \pmod{p^{\alpha}},$$
$$(g + pt_0)^{\delta} \equiv 1 \pmod{p},$$
因此，由指数的性质可知$\delta_p(g + pt_0) \mid \delta$，即$p - 1 \mid \delta$。另一方面，由$\delta$的定义及第一节定理 2 的推论，有$\delta \mid \varphi(p^{\alpha}) = p^{\alpha-1}(p - 1)$，所以
$$\delta = p^{r-1}(p - 1)，1 \le r \le \alpha,$$
即
$$(g + pt)^{p^{r-1}(p-1)} \equiv 1 \pmod{p^{\alpha}}。 \tag{12}$$
由式(10)，有
$$(g + pt)^{p^{r-1}(p-1)} = 1 + p^r y_{r-1},$$
所以，由上式及式(12)推出
$$1 + p^r y_{r-1} \equiv 1 \pmod{p^{\alpha}},$$
$$p^r y_{r-1} \equiv 0 \pmod{p^{\alpha}}。$$
由此及式(11)得到$r \ge \alpha$。所以$r = \alpha$，即$g + pt_0$是模p^{α}的原根。证毕。

引理 4 设p是奇素数，$\alpha \ge 1$，则模 $2p^{\alpha}$有原根。

证明 设g是模p^{α}的原根，则$g + p^{\alpha}$也是模p^{α}的原根，以g_1表示g与$g + p^{\alpha}$中的奇数，则
$$g_1^{\varphi(p^{\alpha})} \equiv 1 \pmod{p^{\alpha}}，g_1 \equiv 1 \pmod{2},$$
因为$(2, p) = 1$，$\varphi(p^{\alpha}) = \varphi(2p^{\alpha})$，所以
$$g_1^{\varphi(2p^{\alpha})} \equiv 1 \pmod{2p^{\alpha}}。 \tag{13}$$
我们指出，不存在正整数$r < \varphi(2p^{\alpha})$，使得
$$g_1^{\,r} \equiv 1 \pmod{2p^{\alpha}}。$$
否则，由上式得到
$$(g_1, p^{\alpha}) = 1，g_1^{\,r} \equiv 1 \pmod{p^{\alpha}},$$
从而g_1不能是模p^{α}的原根。

以上证明了$\delta_{2p^{\alpha}}(g_1) = \varphi(2p^{\alpha})$，即$g_1$是模 $2p^{\alpha}$的原根。证毕。

定理 2 设p是奇素数，$m = 2，4，p^{\alpha}，2p^{\alpha}$，则模$m$有原根。

证明 由引理 3 和引理 4，只需证明模 2 与模 4 有原根，这容易验证：1 是模 2 的原根，3 是模 4 的原根。证毕。

定理 3 设$m > 1$，$\varphi(m)$的所有不同的素因数是$p_1, p_2, \cdots, p_k$，$(g, m) = 1$，则g是模m的原根的充要条件是

$$g^{\frac{\varphi(m)}{p_i}} \not\equiv 1 \pmod{m},\quad 1 \le i \le k。\tag{14}$$

证明 (ⅰ) 必要性是显然的。

(ⅱ) 设式(14)成立。记$\delta = \delta_m(g)$，由第一节定理 2 推论，有$\delta \mid \varphi(m)$。若$\delta < \varphi(m)$，则$\dfrac{\varphi(m)}{\delta} > 1$，所以，必有某个$p_i$（$1 \le i \le k$），使得$p_i \mid \dfrac{\varphi(m)}{\delta}$，因此

$$\delta \,\Big|\, \frac{\varphi(m)}{p_i},\quad g^{\frac{\varphi(m)}{p_i}} \equiv 1 \pmod{m},$$

这与式(14)矛盾。因此$\delta = \varphi(m)$，即 g 是模 m 的原根。证毕。

例 1 求模 7 的原根。

解 由第一节例题 1 可知模 7 有两个原根 3 和 5。

例 2 已知 5 是模 23 的原根，解同余方程

$$x^8 \equiv 18 \pmod{23}。\tag{15}$$

解 由第一节定理 1，$5^i \pmod{23}$（$i = 0, 1, 2, \cdots, 21$）构成模 23 的简化系，列表为

i	0	1	2	3	4	5	6	7	8	9	10
$5^i \pmod{23}$	1	5	2	10	4	20	8	17	16	11	9
i	11	12	13	14	15	16	17	18	19	20	21
$5^i \pmod{23}$	22	18	21	13	19	3	15	6	7	12	14

由上表可知 $5^{12} \equiv 18 \pmod{23}$。

设$x \equiv 5^y \pmod{23}$，$0 \le y \le 22$，则由第一节定理 2，方程(15)等价于

$$8y \equiv 12 \pmod{22}。\tag{16}$$

因为$(8, 22) = 2 \mid 12$，所以方程(16)有两个解：

$$y_1 \equiv 7，\ y_2 \equiv 18 \pmod{22}。$$

因此，方程(15)有两个解

$$x_1 \equiv 5^7 \equiv 17，\quad x_2 \equiv 5^{18} \equiv 6 \pmod{23}。$$

注：若模m有原根g，则模m的简化剩余系$A = \{a_1, a_2, \cdots, a_{\varphi(m)}\}$与集合$B = \{\, g^i;\ 1 \le i \le \varphi(m) \,\}$有一个一一对应关系，即，对于任意的$a_0 \in A$，存在唯一的$g^{i_0} \in B$，使得$a_0 \equiv g^{i_0} \pmod{m}$。此时，称$i_0$是$a_0$对模$m$的以$g$

为底的指标，记为$i_0 = \mathrm{ind}_g a_0$。从例 2 看出，利用指标的概念，我们可以将求解指数同余方程$x^n \equiv a \pmod{m}$的问题转化为求解线性同余方程$n\,\mathrm{ind}_g x \equiv \mathrm{ind}_g a \pmod{\varphi(m)}$。

习 题 二

1. 求模 29 的最小正原根。

2. 分别求模 29^3和模 $2\cdot29^3$的原根。

3. 解同余方程：$x^{12} \equiv 16 \pmod{17}$。

4. 设 p 和 $q = 4p + 1$ 都是素数，证明：2 是模 q 的一个原根。

5. 设$m \geq 3$，g_1和g_2都是模m的原根，则$g = g_1g_2$不是模m的原根。

6. 设 p 是奇素数，证明：当且仅当 $p - 1 \nmid n$ 时，有

$$\boxed{1^n + 2^n + \cdots + (p-1)^n \equiv 0 \pmod{p}}。$$