第 5 章

原根与指标

本章将进一步讨论同余式

$$x^n \equiv a \pmod{m}. \tag{5.1}$$

为此, 需讨论模 m 指数和原根, 以及指标.

5.1 指数及其基本性质

5.1.1 指数

设 $m > 1$ 是整数, a 是与 m 互素的正整数. 根据定理2.4.1 (欧拉定理), 有

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

当然, 要问该 $\varphi(m)$ 是否是使得上式成立的最小正整数以及这个最小正整数具有哪些性质.

定义 5.1.1 设 $m > 1$ 是整数, a 是与 m 互素的正整数, 则使得

$$a^e \equiv 1 \pmod{m} \tag{5.2}$$

成立的最小正整数 e 叫作 a 对模 m 的**指数**, 记作 $\mathrm{ord}_m(a)$.

如果 a 对模 m 的指数是 $\varphi(m)$, 则 a 叫作模 m 的**原根**.

注 1 根据定义5.1.1, 只能逐个计算

$$a^k \pmod{m}, \quad k = 1, 2, \cdots, e \tag{5.3}$$

来确定 a 模 m 的指数 $e = \mathrm{ord}_m(a)$.

注 2 指数 $\mathrm{ord}_m(a)$ 是序列 $u = \{u_k = a^k \mod m \mid k \geqslant 1\}$ 的周期 $p(u)$(见定义B.0.1).

例 5.1.1 设整数 $m = 7$, 这时 $\varphi(7) = 6$. 有

$$1^1 \equiv 1, \qquad 2^3 = 8 \equiv 1, \qquad 3^3 = 27 \equiv -1,$$
$$4^3 \equiv (-3)^3 \equiv 1, \quad 5^3 \equiv (-2)^3 \equiv -1, \quad 6^2 \equiv (-1)^2 \equiv 1 \pmod{7}.$$

列成表为

a	1	2	3	4	5	6
$\mathrm{ord}_m(a)$	1	3	6	3	6	2

因此, 3、5是模7的原根. 但2、4、6不是模7的原根.

例 5.1.2　设整数 $m=14=2\cdot 7$, 这时 $\varphi(14)=6$. 有

$$1^1\equiv 1,\qquad 3^3=27\equiv -1,\qquad 5^3=125\equiv -1,$$
$$9^3\equiv(-5)^3\equiv 1,\quad 11^3\equiv(-3)^3\equiv 1,\quad 13^2\equiv(-1)^2\equiv 1\ (\mathrm{mod}\ 14).$$

列成表为

a	1	3	5	9	11	13
$\mathrm{ord}_m(a)$	1	6	6	3	3	2

因此, 3、5是模14的原根. 但9、11、13 不是模14的原根.

例 5.1.3　设整数 $m=15=3\cdot 5$, 这时 $\varphi(15)=8$. 有

$$1^1\equiv 1,\qquad 2^4=16\equiv 1,\qquad 4^2=16\equiv 1,$$
$$7^2=49\equiv 4,\qquad 7^4\equiv 16\equiv 1,\qquad 8^4\equiv(-7)^4\equiv 1,$$
$$11^2\equiv(-4)^2\equiv 1,\quad 13^4\equiv(-2)^4\equiv 1,\quad 14^2\equiv(-1)^2\equiv 1\ (\mathrm{mod}\ 15).$$

列成表为

a	1	2	4	7	8	11	13	14
$\mathrm{ord}_m(a)$	1	4	2	4	4	2	4	2

因此, 没有模15的原根.

例 5.1.4　设整数 $m=9=3^2$, 这时 $\varphi(9)=6$. 有

$$1^1\equiv 1,\qquad 2^3=8\equiv -1,\qquad 4^3=64\equiv 1,$$
$$5^3\equiv(-4)^3\equiv -1,\quad 7^3\equiv(-2)^3\equiv 1,\quad 8^2\equiv(-1)^2\equiv 1\ (\mathrm{mod}\ 9).$$

列成表为

a	1	2	4	5	7	8
$\mathrm{ord}_m(a)$	1	6	3	6	3	2

因此, 2、5是模9的原根.

例 5.1.5　设整数 $m=8=2^3$, 这时 $\varphi(8)=4$. 有

$$1^1\equiv 1,\ 3^2=9\equiv 1,\ 5^2=25\equiv 1,\ 7^2\equiv(-1)^2\equiv 1\ (\mathrm{mod}\ 8).$$

列成表为

a	1	3	5	7
$\mathrm{ord}_m(a)$	1	2	2	2

因此, 没有模8的原根.

例 5.1.6　证明: 5是模3及模6的原根, 也是模 3^2、$2\cdot 3^2$ 的原根.

因为 $\varphi(3)=2$, 且

$$5\equiv -1,\ 5^2\equiv 1\ (\mathrm{mod}\ 3);$$

同样, 因为 $\varphi(6)=2$, 且

$$5\equiv -1,\ 5^2\equiv 1\ (\mathrm{mod}\ 3^2);$$

类似地, 因为 $\varphi(3^2)=6$, 且

$$5\equiv 5,\ 5^2\equiv 7,\ 5^3\equiv 8\equiv -1, 5^4\equiv 4,\ 5^5\equiv 2,\ 5^6\equiv 1\ (\mathrm{mod}\ 3^2);$$

对于模 $2\cdot 3^2$, 因为 $(5,2)=1$, 所以有

$$5\equiv 5,\ 5^2\equiv 7,\ 5^3\equiv 8\equiv -1, 5^4\equiv 4,\ 5^5\equiv 2,\ 5^6\equiv 1\ (\mathrm{mod}\ 2\cdot 3^2).$$

因此, 结论成立.

5.1.2 指数的基本性质

现在讨论指数的性质. 类似于周期序列 u 的最小周期 $p(u)$ (见定义B.0.1), 有

定理 5.1.1 设 $m>1$ 是整数, a 是与 m 互素的整数, 则整数 d 使得

$$a^d\equiv 1\ (\mathrm{mod}\ m) \tag{5.4}$$

的充分必要条件是

$$\mathrm{ord}_m(a)\mid d. \tag{5.5}$$

证 充分性. 设式 (5.5) 成立, 即 $\mathrm{ord}_m(a)\mid d$, 那么存在整数 q 使得 $d=q\cdot \mathrm{ord}_m(a)$. 因此, 有

$$a^d=\left[a^{\mathrm{ord}_m(a)}\right]^q\equiv 1\ (\mathrm{mod}\ m).$$

必要性. 反证法. 如果式 (5.5) 不成立, 即 $\mathrm{ord}_m(a)\nmid d$, 则由欧几里得除法 (定理1.1.9), 存在整数 q、r 使得

$$d=q\cdot \mathrm{ord}_m(a)+r,\qquad 0<r<\mathrm{ord}_m(a).$$

从而,

$$a^r\equiv \left[a^{\mathrm{ord}_m(a)}\right]^q\cdot a^r=a^d\equiv 1\ (\mathrm{mod}\ m).$$

这与 $\mathrm{ord}_m(a)$ 的最小性矛盾. 故式 (5.5) 成立. 证毕.

推论1 设 $m>1$ 是整数, a 是与 m 互素的整数, 则

$$\mathrm{ord}_m(a)\mid \varphi(m). \tag{5.6}$$

证 根据欧拉定理 (定理2.4.1), 有

$$a^{\varphi(m)}\equiv 1\ (\mathrm{mod}\ m).$$

由定理5.1.1, 有式 (5.6). 证毕.

注 根据推论1的式 (5.6) , 整数 a 模 m 的指数 $\mathrm{ord}_m(a)$ 是 $\varphi(m)$ 的因数, 所以可以在 $\varphi(m)$ 的因数中求 $\mathrm{ord}_m(a)$. 与根据定义5.1.1 求指数 $\mathrm{ord}_m(a)$ 式 (5.3) 相比, 运算效率提高了许多.

例 5.1.7 求整数5模17的指数 $\mathrm{ord}_{17}(5)$.

解 因为 $\varphi(17)=16$, 所以只需对16的因数 $d=1,\ 2,\ 4,\ 8,\ 16$, 计算 $a^d\ (\mathrm{mod}\ m)$. 因为

$$5^1\equiv 5,\ 5^2=25\equiv 8,\ 5^4\equiv 64\equiv 13\equiv -4, 5^8\equiv (-4)^2\equiv 16\equiv -1,\ 5^{16}\equiv (-1)^2\equiv 1\ (\mathrm{mod}\ 17),$$

所以 $\mathrm{ord}_{17}(5)=16$. 这说明5是模17的原根.

推论2　设p是奇素数, 且$\dfrac{p-1}{2}$也是素数. 如果a是一个模p不为0、1、-1的整数, 则

$$\mathrm{ord}_p(a)=\frac{p-1}{2}\ \text{或}\ p-1.$$

证　根据欧拉定理 (定理2.4.1), 有

$$a^{\varphi(p)}\equiv 1\ (\mathrm{mod}\ p).$$

根据推论1, 整数a模p的指数$\mathrm{ord}_p(a)$是$\varphi(p)=p-1=2\cdot\dfrac{p-1}{2}$的因数, 但$\mathrm{ord}_m(a)\neq 2$,所以

$$\mathrm{ord}_p(a)=\frac{p-1}{2}\ \text{或}\ p-1.$$

证毕.

性质 5.1.1　设$m>1$是整数, a是与m互素的整数.

(i) 若$b\equiv a\ (\mathrm{mod}\ m)$, 则$\mathrm{ord}_m(b)=\mathrm{ord}_m(a)$.

(ii) 设a^{-1}使得$a^{-1}\cdot a\equiv 1\ (\mathrm{mod}\ m)$, 则$\mathrm{ord}_m(a^{-1})=\mathrm{ord}_m(a)$.

证　(i) 若$b\equiv a\ (\mathrm{mod}\ m)$, 则

$$b^{\mathrm{ord}_m(a)}\equiv a^{\mathrm{ord}_m(a)}\equiv 1\ (\mathrm{mod}\ m),$$

根据定理5.1.1式 (5.5), 有$\mathrm{ord}_m(b)\mid\mathrm{ord}_m(a)$.

同样, 有$\mathrm{ord}_m(a)\mid\mathrm{ord}_m(b)$. 故$\mathrm{ord}_m(b)=\mathrm{ord}_m(a)$.

(ii) 因为

$$(a^{-1})^{\mathrm{ord}_m(a)}\equiv\left[a^{\mathrm{ord}_m(a)}\right]^{-1}\equiv 1\ (\mathrm{mod}\ m),$$

根据定理5.1.1的式 (5.5), 有$\mathrm{ord}_m(a^{-1})\mid\mathrm{ord}_m(a)$.

同样, 有$\mathrm{ord}_m(a)\mid\mathrm{ord}_m(a^{-1})$. 故$\mathrm{ord}_m(a^{-1})=\mathrm{ord}_m(a)$.　证毕.

例 5.1.8　整数39模17的指数为$\mathrm{ord}_{17}(39)=\mathrm{ord}_{17}(5)=16$. 整数7模17的指数为16. 因为$5^{-1}\equiv 7\ (\mathrm{mod}\ m)$.

定理 5.1.2　设$m>1$是整数, a是与m互素的整数, 则

$$1=a^0,\ a,\ \cdots,\ a^{\mathrm{ord}_m(a)-1}\tag{5.7}$$

模m两两不同余. 特别地, 当a是模m的原根, 即$\mathrm{ord}_m(a)=\varphi(m)$时, 这$\varphi(m)$个数

$$1=a^0,\ a,\ \cdots,\ a^{\varphi(m)-1}\tag{5.8}$$

组成模m的简化剩余系.

证　反证法. 如果式 (5.7) 中有两个数模m同余, 则存在整数$0\leqslant k,\ l<\mathrm{ord}_m(a)$使得

$$a^k\equiv a^l\ (\mathrm{mod}\ m).$$

不妨设$k>l$. 则由$(a,m)=1$和定理2.1.8, 得

$$a^{k-l}\equiv 1\ (\mathrm{mod}\ m).$$

但$0<k-l<\mathrm{ord}_m(a)$.这与$\mathrm{ord}_m(a)$的最小性矛盾. 因此, 结论成立.

再设a是模m的原根, 即$\mathrm{ord}_m(a)=\varphi(m)$, 则有$\varphi(m)$个数即式 (5.8), 也即

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

模m两两不同余. 根据定理2.3.3, 这$\varphi(m)$个数组成模m的简化剩余系. 证毕.

注 当模m有原根g时, 简化剩余a可表示为g^d. 基于这一表示即$a=g^d$, 可以简化一些问题的讨论, 如n次同余式(参见定理5.3.4)$x^n\equiv b\pmod m$. 进一步, 通过建立指数表$a\leftrightarrow g^d$, 也可以空间换时间的方式来提高运算效率, 如计算(参见例5.3.1)

$$a\cdot b\pmod m\equiv g^{\mathrm{ind}_g a}\cdot g^{\mathrm{ind}_g b}\pmod m=g^{\mathrm{ind}_g a+\mathrm{ind}_g b}\pmod m$$

例 5.1.9 整数$\{5^k|k=0,\cdots,15\}$组成模17的简化剩余系. 进一步, 查表计算$7\cdot 13\pmod{17}$.

解 作计算如下:

$$\begin{aligned}
&5^0\equiv 1, && 5^1\equiv 5, && 5^2=25\equiv 8,\\
&5^3\equiv 5\cdot 8\equiv 6, && 5^4\equiv 8^2\equiv 13, && 5^5\equiv 5\cdot 13\equiv 14,\\
&5^6\equiv 6^2\equiv 2, && 5^7\equiv 5\cdot 2\equiv 10, && 5^8\equiv 5\cdot 10\equiv 50\equiv 16\equiv -1\\
&5^9\equiv 5\cdot(-1)\equiv 12, && 5^{10}\equiv(-1)\cdot 8\equiv 9, && 5^{11}\equiv(-1)\cdot 6\equiv 11,\\
&5^{12}\equiv(-1)\cdot 13\equiv 4, && 5^{13}\equiv(-1)\cdot 14\equiv 3, && 5^{14}\equiv(-1)\cdot 2\equiv 15,\\
&5^{15}\equiv(-1)\cdot 10\equiv 7 \pmod{17}.
\end{aligned}$$

列表为

5^0	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}
1	5	8	6	13	14	2	10	16	12	9	11	4	3	15	7

进一步, 有

$$7\cdot 13\equiv 5^{15}\cdot 5^4=5^{19}\equiv 5^3\equiv 6\pmod{17}.$$

定理 5.1.3 设$m>1$是整数, a是与m互素的整数, 则

$$a^d\equiv a^k\pmod m$$

的充分必要条件是

$$d\equiv k\pmod{\mathrm{ord}_m(a)}.$$

证 根据欧几里得除法(定理1.1.9), 存在整数q、r和q'、r'使得

$$\begin{aligned}
d&=q\cdot\mathrm{ord}_m(a)+r,\quad 0\leqslant r<\mathrm{ord}_m(a).\\
k&=q'\cdot\mathrm{ord}_m(a)+r',\quad 0\leqslant r'<\mathrm{ord}_m(a).
\end{aligned}$$

又$a^{\mathrm{ord}_m(a)}\equiv 1\pmod m$, 故

$$a^d\equiv(a^{\mathrm{ord}_m(a)})^q\cdot a^r\equiv a^r,\quad a^k\equiv a^{r'}\pmod m.$$

必要性. 若$a^d\equiv a^k$, 则

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

由定理5.1.2, 得到$r=r'$. 故$d\equiv k\pmod{\mathrm{ord}_m(a)}$.

充分性. 若$d\equiv k\pmod{\mathrm{ord}_m(a)}$, 则

$$r=r',\quad a^d\equiv a^k\pmod m.$$

因此, 定理成立. 证毕.

例 5.1.10　$2^{1\,000\,000} \equiv 2^{10} \equiv 100 \pmod{231}$.

因为整数2模231的指数为 $\mathrm{ord}_{231}(2) = 30$, $1\,000\,000 \equiv 10 \pmod{30}$.

例 5.1.11　$2^{2002} \equiv 2^1 \equiv 2 \pmod 7$.

因为整数2模7的指数为 $\mathrm{ord}_7(2) = 3$,$2002 \equiv 1 \pmod 3$.

定理 5.1.4　设 $m > 1$ 是整数, a 是与 m 互素的整数. 设 d 为非负整数, 则

$$\mathrm{ord}_m(a^d) = \frac{\mathrm{ord}_m(a)}{(d, \mathrm{ord}_m(a))}. \tag{5.9}$$

证　因为

$$a^{d\ \mathrm{ord}_m\left(a^d\right)} = \left(a^d\right)^{\mathrm{ord}_m\left(a^d\right)} \equiv 1 \pmod m,$$

根据定理5.1.1, $\mathrm{ord}_m(a) \mid d\ \mathrm{ord}_m\left(a^d\right)$. 从而

$$\frac{\mathrm{ord}_m(a)}{(d, \mathrm{ord}_m(a))} \mid \mathrm{ord}_m(a^d) \cdot \frac{d}{(d, \mathrm{ord}_m(a))}.$$

因为 $\left(\dfrac{\mathrm{ord}_m(a)}{(d, \mathrm{ord}_m(a))}, \dfrac{d}{(d, \mathrm{ord}_m(a))}\right) = 1$, 根据定理1.3.11之推论,

$$\frac{\mathrm{ord}_m(a)}{(d, \mathrm{ord}_m(a))} \mid \mathrm{ord}_m(a^d).$$

另一方面, 有

$$\left(a^d\right)^{\frac{\mathrm{ord}_m(a)}{(d, \mathrm{ord}_m(a))}} = \left(a^{\mathrm{ord}_m(a)}\right)^{\frac{d}{(d, \mathrm{ord}_m(a))}} \equiv 1 \pmod m,$$

根据定理5.1.1,

$$\mathrm{ord}_m\left(a^d\right) \mid \frac{\mathrm{ord}_m(a)}{(d, \mathrm{ord}_m(a))}.$$

因此, 有式 (5.9). 证毕.

例 5.1.12　整数 $5^2 \equiv 8 \pmod{17}$ 模17的指数为 $\mathrm{ord}_{17}\left(5^2\right) = \dfrac{\mathrm{ord}_{17}(5)}{(2, \mathrm{ord}_{17}(5))} = 8$.

推论 1　设 $m > 1$ 是整数, g 是模 m 的原根. 设 $d \geqslant 0$ 为整数, 则 g^d 是模的原根当且仅当 $(d, \varphi(m)) = 1$.

证　根据定理5.1.4的式 (5.9), 有

$$\mathrm{ord}_m\left(g^d\right) = \frac{\mathrm{ord}_m(g)}{(d, \mathrm{ord}_m(g))} = \frac{\varphi(m)}{(d, \varphi(m))}.$$

因此, g^d 是模的原根, 即 $\mathrm{ord}_m\left(g^d\right) = \varphi(m)$ 当且仅当 $(d, \varphi(m)) = 1$. 证毕.

推论 2　设 $m > 1$ 是整数, a 是与 m 互素的整数. 设 $k \mid \mathrm{ord}_m(a)$ 为正整数, 则使得

$$\mathrm{ord}_m(a^d) = k, \quad 1 \leqslant d \leqslant \mathrm{ord}_m(a)$$

正整数 d 满足 $\dfrac{\mathrm{ord}_m(a)}{k} \mid d$, 且这样 d 的个数为 $\varphi(k)$.

证　根据定理5.1.4, 有

$$k = \mathrm{ord}_m\left(a^d\right) = \frac{\mathrm{ord}_m(a)}{(d, \mathrm{ord}_m(a))}.$$

所以

$$(d, \mathrm{ord}_m(a)) = \frac{\mathrm{ord}_m(a)}{k}.$$

因此, $\dfrac{\mathrm{ord}_m(a)}{k} \mid d$. 再令

$$d = q \cdot \frac{\mathrm{ord}_m(a)}{k}, \quad 1 \leqslant q \leqslant k.$$

由

$$\mathrm{ord}_m\left(a^d\right) = \frac{\mathrm{ord}_m(a)}{(d, \mathrm{ord}_m(a))} = \frac{\mathrm{ord}_m(a)}{\left(q \cdot \dfrac{\mathrm{ord}_m(a)}{k}, \mathrm{ord}_m(a)\right)} = \frac{k}{(q,k)},$$

得到$\mathrm{ord}_m(a^d) = k$的充要条件是$(q,k) = 1$. 因此, d的个数为$\varphi(k)$. 证毕.

定理 5.1.5 设$m > 1$是整数. 如果模m存在一个原根g, 则模m有$\varphi(\varphi(m))$个不同的原根.

证 设g是模m的一个原根. 根据定理5.1.2的式 (5.8), $\varphi(m)$个整数

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

构成模m的一个简化剩余系. 又根据定理5.1.4之推论, g^d是模m的原根当且仅当 $(d, \varphi(m)) = 1$. 因为这样的d共有$\varphi(\varphi(m))$个, 所以模m有$\varphi(\varphi(m))$个不同的原根. 证毕.

推论 设$m > 1$是整数, 且模m存在一个原根. 设

$$\varphi(m) = p_1^{\alpha_1} \cdots p_s^{\alpha_s}, \quad \alpha_i > 0,\ i = 1, \cdots, s,$$

则整数a, $(a,m) = 1$是模m原根的概率是

$$\frac{\varphi(\varphi(m))}{\varphi(m)} = \prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right). \tag{5.10}$$

证 根据定理5.1.5, 整数a, $(a,m) = 1$是模m 原根的概率是

$$\frac{\varphi(\varphi(m))}{\varphi(m)}.$$

又根据欧拉函数$\varphi(m)$的性质以及$\varphi(m)$的素因数分解表达式, 有

$$\frac{\varphi(\varphi(m))}{\varphi(m)} = \prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right).$$

因此, 结论成立. 证毕.

例 5.1.13 求出模17的所有原根.

解 由例5.1.7可知, 5是模17的原根. 再由定理5.1.5, 得到$\varphi(\varphi(17)) = \varphi(16) = 8$个整数$5,\ 5^3 \equiv 6,\ 5^5 \equiv 14,\ 5^7 \equiv 10,\ 5^9 \equiv 12,\ 5^{11} \equiv 11,\ 5^{13} \equiv 3,\ 5^{15} \equiv 7 \pmod{17}$是模17的全部原根.

5.1.3 大指数的构造

本节讨论如何构造大指数.

定理 5.1.6 设$m > 1$是整数, a、b都是与m互素的整数. 如果$(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$, 则

$$\mathrm{ord}_m(a \cdot b) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b). \tag{5.11}$$

反之亦然.

证 因为$(a,m) = 1$, $(b,m) = 1$, 所以$(a \cdot b, m) = 1$, 且存在$\mathrm{ord}_m(a \cdot b)$.

因为

$$\begin{aligned} a^{\mathrm{ord}_m(b)\cdot\mathrm{ord}_m(a\cdot b)} &\equiv \left(a^{\mathrm{ord}_m(b)}\right)^{\mathrm{ord}_m(a\cdot b)}\cdot\left(b^{\mathrm{ord}_m(b)}\right)^{\mathrm{ord}_m(a\cdot b)} \\ &\equiv \left((ab)^{\mathrm{ord}_m(a\cdot b)}\right)^{\mathrm{ord}_m(b)} \\ &\equiv 1 \pmod m, \end{aligned}$$

因此, $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(b)\cdot\mathrm{ord}_m(a\cdot b)$. 但 $(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$, 根据定理1.3.11之推论, 得到 $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(a\cdot b)$.

同理, $\mathrm{ord}_m(b) \mid \mathrm{ord}_m(a\cdot b)$. 再由 $(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$ 及定理1.4.4, 得到

$$\mathrm{ord}_m(a)\cdot\mathrm{ord}_m(b) \mid \mathrm{ord}_m(a\cdot b).$$

另一方面, 有

$$(ab)^{\mathrm{ord}_m(a)\cdot\mathrm{ord}_m(b)} = \left(a^{\mathrm{ord}_m(a)}\right)^{\mathrm{ord}_m(b)}\cdot\left(b^{\mathrm{ord}_m(b)}\right)^{\mathrm{ord}_m(a)} \equiv 1 \pmod m,$$

从而 $\mathrm{ord}_m(ab) \mid \mathrm{ord}_m(a)\cdot\mathrm{ord}_m(b)$. 故

$$\mathrm{ord}_m(ab) = \mathrm{ord}_m(a)\cdot\mathrm{ord}_m(b).$$

反过来, 如果 $\mathrm{ord}_m(a\cdot b) = \mathrm{ord}_m(a)\cdot\mathrm{ord}_m(b)$, 那么由

$$(ab)^{[\mathrm{ord}_m(a),\mathrm{ord}_m(b)]} = a^{[\mathrm{ord}_m(a),\mathrm{ord}_m(b)]}\cdot b^{[\mathrm{ord}_m(a),\mathrm{ord}_m(b)]} \equiv 1 \pmod m,$$

推得

$$\mathrm{ord}_m(a\cdot b) \mid [\mathrm{ord}_m(a), \mathrm{ord}_m(b)],$$

即

$$\mathrm{ord}_m(a)\cdot\mathrm{ord}_m(b) \mid [\mathrm{ord}_m(a), \mathrm{ord}_m(b)].$$

因此,

$$(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1.$$

结论成立. 证毕.

注　对于模 m, 不一定有

$$\mathrm{ord}_m(a\cdot b) = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)]$$

成立. 例如, 由例5.1.2,

$$\mathrm{ord}_{10}(3\cdot 3) = 2 \neq [\mathrm{ord}_{10}(3), \mathrm{ord}_{10}(3)] = 4,$$

$$\mathrm{ord}_{10}(3\cdot 7) = 1 \neq [\mathrm{ord}_{10}(3), \mathrm{ord}_{10}(7)] = 4.$$

但有

$$\mathrm{ord}_{10}(7\cdot 9) = 4 = [\mathrm{ord}_{10}(7), \mathrm{ord}_{10}(9)] = 4.$$

例 5.1.14　*求模71的原根.*

解　计算整数2模71的指数为 $\mathrm{ord}_{71}(2) = 35$; 因此, 整数 -2 为模71的原根, 因为 -2 模71的指数为 $\mathrm{ord}_{71}(-2) = \mathrm{ord}_{71}(-1)\cdot\mathrm{ord}_{71}(2) = 70$.

定理 5.1.7　*设 m、n 都是大于 1 的整数, a 是与 m 互素的整数, 则*

(i) *若 $n \mid m$, 则 $\mathrm{ord}_n(a) \mid \mathrm{ord}_m(a)$.*

(ii) 若 $(m,n)=1$, 则

$$\mathrm{ord}_{mn}(a)=[\mathrm{ord}_m(a),\mathrm{ord}_n(a)]. \tag{5.12}$$

证 (i) 根据 $\mathrm{ord}_m(a)$ 的定义, 有

$$a^{\mathrm{ord}_m(a)}\equiv 1 \pmod m.$$

因此, 当 $n\mid m$ 时, 可推出

$$a^{\mathrm{ord}_m(a)}\equiv 1 \pmod n.$$

根据定理5.1.1, 得到

$$\mathrm{ord}_n(a)\mid \mathrm{ord}_m(a).$$

(ii) 由 (i) 有

$$\mathrm{ord}_m(a)\mid \mathrm{ord}_{mn}(a),\quad \mathrm{ord}_n(a)\mid \mathrm{ord}_{mn}(a),$$

根据定理1.4.5, 有 $[\mathrm{ord}_m(a),\mathrm{ord}_n(a)]\mid \mathrm{ord}_{mn}(a)$.

又由

$$a^{[\mathrm{ord}_m(a),\mathrm{ord}_n(a)]}\equiv 1 \pmod m,\quad a^{[\mathrm{ord}_m(a),\mathrm{ord}_n(a)]}\equiv 1 \pmod n,$$

及定理2.1.12 可推出

$$a^{[\mathrm{ord}_m(a),\mathrm{ord}_n(a)]}\equiv 1 \pmod{mn}.$$

从而, $\mathrm{ord}_{mn}(a)\mid [\mathrm{ord}_m(a),\mathrm{ord}_n(a)]$. 故式 (5.12) 成立. 证毕.

推论1 设 p、q 是两个不同的奇素数, a 是与 $p\cdot q$ 互素的整数, 则

$$\mathrm{ord}_{p\cdot q}(a)=[\mathrm{ord}_p(a),\mathrm{ord}_q(a)]\mid [p-1,q-1]. \tag{5.13}$$

证 由定理5.1.7 (ii) 和 $\mathrm{ord}_p(a)\mid p-1$, $\mathrm{ord}_q(a)\mid q-1$ 即得.

推论2 设 p, $q=2p-1$ 是两个不同的奇素数, a 是与 $p\cdot q$ 互素的整数, 则

$$\mathrm{ord}_{p\cdot q}(a)=[\mathrm{ord}_p(a),\mathrm{ord}_q(a)]\mid q-1. \tag{5.14}$$

证 由推论1 和 $[p-1,q-1]=q-1$ 即得.

例 5.1.15 设 p, q 是不同奇素数, $n=p\cdot q$, a 是与 n 互素的整数. 如果整数 e 满足

$$1<e<\varphi(n),\ (e,\varphi(n))=1, \tag{5.15}$$

那么存在整数 $d=d_a$, $1\leqslant d<\mathrm{ord}_{pq}(a)$, 使得

$$e\cdot d\equiv 1 \pmod{\mathrm{ord}_{pq}(a)}. \tag{5.16}$$

而且, 对于整数

$$a^e\equiv c \pmod n,\quad 1\leqslant c<n, \tag{5.17}$$

有

$$c^d\equiv a \pmod n. \tag{5.18}$$

证 因为 $(e,\varphi(n))=1$, 又根据定理5.1.1之推论1, $\mathrm{ord}_{pq}(a)\mid\varphi(n)$, 所以 $(e,\mathrm{ord}_{pq}(a))=1$. 根据定理2.3.5, 存在整数 $d=d_a$, $1\leqslant d<\mathrm{ord}_{pq}(a)$, 使得式 (5.16) 成立, 即

$$e\cdot d\equiv 1 \pmod{\mathrm{ord}_{pq}(a)}.$$

因此, 存在一个正整数 k 使得 $e\cdot d=1+k\ \mathrm{ord}_{pq}(a)$.

现在, 根据指数的定义, 得到

$$a^{\mathrm{ord}_p(a)} \equiv 1 \pmod{p}. \tag{5.19}$$

根据定理5.1.6之推论1, $\dfrac{\mathrm{ord}_{pq}(a)}{\mathrm{ord}_p(a)}$ 为整数. 在式 (5.19) 的两端作 $k\dfrac{\mathrm{ord}_{pq}(a)}{\mathrm{ord}_p(a)}$ 次幂, 并乘以 a 得到

$$a^{1+k\ \mathrm{ord}_{pq}(a)} \equiv a \pmod{p},$$

即

$$a^{ed} \equiv a \pmod{p}.$$

同理,

$$a^{ed} \equiv a \pmod{q}.$$

因为 p 和 q 是不同的素数, 根据定理2.1.12 ,

$$a^{ed} \equiv a \pmod{n},$$

因此,

$$c^d \equiv (a^e)^d \equiv a \pmod{n}.$$

即式 (5.18) 成立. 证毕.

推论 3　设 m 是大于 1 的整数, a 是与 m 互素的整数, 则当 m 的标准分解式为

$$m = 2^n \cdot p_1^{\alpha_1} \cdots p_k^{\alpha_k}$$

时, 有

$$\mathrm{ord}_m(a) = \left[\mathrm{ord}_{2^n}(a), \mathrm{ord}_{p_1^{\alpha_1}}(a), \cdots, \mathrm{ord}_{p_k^{\alpha_k}}(a)\right]. \tag{5.20}$$

定理 5.1.8　*设 m、n 都是大于 1 的整数, 且 $(m,n)=1$. 则对与 mn 互素的任意整数 a_1、a_2, 存在整数 a 使得*

$$\mathrm{ord}_{mn}(a) = \left[\mathrm{ord}_m(a_1), \mathrm{ord}_n(a_2)\right]. \tag{5.21}$$

证　考虑同余式组

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

根据中国剩余定理 (定理3.2.1), 这个同余式组有唯一解

$$x \equiv a \pmod{mn}.$$

根据性质5.1.1 (i), 有

$$\mathrm{ord}_m(a) = \mathrm{ord}_m(a_1), \quad \mathrm{ord}_n(a) = \mathrm{ord}_n(a_2).$$

因此, 从定理5.1.7 得到,

$$\mathrm{ord}_{mn}(a) = \left[\mathrm{ord}_m(a), \mathrm{ord}_n(a)\right] = \left[\mathrm{ord}_m(a_1), \mathrm{ord}_n(a_2)\right].$$

证毕.

定理 5.1.9　*设 $m>1$ 是整数, 则对与 m 互素的任意整数 a、b, 存在整数 c 使得*

$$\mathrm{ord}_m(c) = \left[\mathrm{ord}_m(a), \mathrm{ord}_m(b)\right]. \tag{5.22}$$

证 根据定理1.6.6, 对于整数$\mathrm{ord}_m(a)$和$\mathrm{ord}_m(b)$,存在整数u、v满足

$$u \mid \mathrm{ord}_m(a), \quad v \mid \mathrm{ord}_m(b), \quad (u,v)=1,$$

使得

$$[\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)] = u \cdot v.$$

现在令

$$s = \frac{\mathrm{ord}_m(a)}{u}, \quad t = \frac{\mathrm{ord}_m(b)}{v},$$

根据定理5.1.4, 有

$$\mathrm{ord}_m(a^s) = \frac{\mathrm{ord}_m(a)}{(s, \mathrm{ord}_m(a))} = u, \quad \mathrm{ord}_m(b^t) = v.$$

再根据定理5.1.6, 得到

$$\mathrm{ord}_m\left(a^s \cdot b^t\right) = \mathrm{ord}_m\left(a^s\right)\mathrm{ord}_m\left(b^t\right) = u \cdot v = [\mathrm{ord}_m(a),\ \mathrm{ord}_m(b)].$$

因此, 取$c = a^s \cdot b^t \pmod m$.即为所求. 证毕.

例 5.1.16 设整数$m=3631$, m是素数, 有$\varphi(3631)=3630=2\cdot 3\cdot 5\cdot 11^2$,以及

$$\begin{aligned}
&\mathrm{ord}_{3631}(2)=605=5\cdot 11^2, && \mathrm{ord}_{3631}(3)=1210=2\cdot 5\cdot 11^2,\\
&\mathrm{ord}_{3631}(5)=363=3\cdot 11^2, && \mathrm{ord}_{3631}(6)=1210=2\cdot 5\cdot 11^2,\\
&\mathrm{ord}_{3631}(7)=33=3\cdot 11, && \mathrm{ord}_{3631}(10)=1815=3\cdot 5\cdot 11^2,\\
&\mathrm{ord}_{3631}(11)=330=2\cdot 3\cdot 5\cdot 11, && \mathrm{ord}_{3631}(12)=1210=2\cdot 5\cdot 11^2,\\
&\mathrm{ord}_{3631}(13)=1815=3\cdot 5\cdot 11^2, && \mathrm{ord}_{3631}(14)=1815=3\cdot 5\cdot 11^2,\\
&\mathrm{ord}_{3631}(15)=3630=2\cdot 3\cdot 5\cdot 11^2, && \mathrm{ord}_{3631}(17)=1210=2\cdot 5\cdot 11^2.
\end{aligned}$$

根据定理5.1.9, 取整数$a=3$, $b=5$以及$u=1210$, $v=3$, 这时$s=1$, $t=11^2$,得整数$c=a^s\cdot b^t=3^1\cdot 5^{121}\equiv 2623 \pmod{3631}$的指数为

$$\mathrm{ord}_{3631}(2623)=\mathrm{ord}_{3631}\left(3^1\right)\cdot\mathrm{ord}_{3631}\left(5^{121}\right)=3630=[\mathrm{ord}_{3631}(3),\mathrm{ord}_{3631}(5)].$$

因此, $c=2623$是模3631的原根.

定理 5.1.10 设$m>1$是整数, $a_1,a_2,\cdots,a_{\varphi(m)}$是模$m$的简化剩余系.$e$是使得

$$a_k^e \equiv 1 \pmod m, \quad 1 \leqslant k \leqslant \varphi(m) \tag{5.23}$$

成立的最小正整数, 则存在整数a使得

$$e=\mathrm{ord}_m(a)=\left[\mathrm{ord}_m(a_1),\mathrm{ord}_m(a_2),\cdots,\mathrm{ord}_m\left(a_{\varphi(m)}\right)\right]. \tag{5.24}$$

证 应用定理5.1.9, 可归纳得到: 存在整数a使得

$$\mathrm{ord}_m(a)=\left[\mathrm{ord}_m(a_1),\mathrm{ord}_m(a_2),\cdots,\mathrm{ord}_m\left(a_{\varphi(m)}\right)\right]$$

现证明$e=\mathrm{ord}_m(a)$. 事实上, 对每个a_k, 有

$$a_k^e \equiv 1 \pmod m$$

根据定理5.1.1, 有$\mathrm{ord}_m(a_k)\mid e$, $1\leqslant k\leqslant\varphi(m)$. 所以

$$\left[\mathrm{ord}_m(a_1),\mathrm{ord}_m(a_2),\cdots,\mathrm{ord}_m\left(a_{\varphi(m)}\right)\right]\mid e.$$

另一方面, 对每个a_k, 有

$$a_k^{\left[\mathrm{ord}_m(a_1),\cdots,\mathrm{ord}_m\left(a_{\varphi(m)}\right)\right]}=\left((a_k)^{\mathrm{ord}_m(a_k)}\right)^{\left[\mathrm{ord}_m(a_1),\cdots,\mathrm{ord}_m\left(a_{\varphi(m)}\right)\right]/\mathrm{ord}_m(a_k)}\equiv 1\ (\mathrm{mod}\ m).$$

根据e的最小性, 有$e\leqslant\left[\mathrm{ord}_m(a_1),\cdots,\mathrm{ord}_m\left(a_{\varphi(m)}\right)\right]$. 因此式 (5.24) 成立. 证毕.

定义 5.1.2　定理5.1.10 中的最小正整数e叫作模m的简化剩余系指数, 记作

$$e=\mathrm{ord}\left((\mathbf{Z}/m\mathbf{Z})^*\right)$$

当$m=p$是素数时, 有

$$e=\mathrm{ord}\left((\mathbf{Z}/p\mathbf{Z})^*\right)=\mathrm{ord}\left((\boldsymbol{F}_p)^*\right)=\varphi(p).$$

5.2　原　　根

5.2.1　模p原根

先讨论m为奇素数p的情形.

先给出模p原根的存在性证明和原根个数.

定理 5.2.1　设p是奇素数, 则模p的原根存在, 且有$\varphi(p-1)$个原根, 其中φ为欧拉函数.

证一 (构造性)　在模p的简化剩余系$1,\ \cdots,\ p-1$中, 记

$$e_r=\mathrm{ord}_p(r),\quad 1\leqslant r\leqslant p-1,$$

$$e=[e_1,\cdots,e_{p-1}].$$

根据定理5.1.8, 存在整数g, 使得

$$g^e\equiv 1\ (\mathrm{mod}\ p).$$

因此, $e\mid\varphi(p)=p-1$. 又因为

$$e_r\mid e,\quad r=1,\cdots,p-1,$$

从而推出同余式

$$x^e\equiv 1\ (\mathrm{mod}\ p)$$

有$p-1$个解

$$x\equiv 1,\ \cdots,\ p-1\ (\mathrm{mod}\ p).$$

根据定理3.4.4, 有$p-1\leqslant e$. 故g的指数为$p-1$, 即g是模p的原根.

最后, 根据定理5.1.4之推论 1, 当g为原根时, $g^d,\ (d,p-1)=1$也是原根, 共有$\varphi(p-1)$个.

证二 (存在性)　设$d\mid p-1$. 用$F(d)$表示模p的简化剩余系中指数为d的元素个数. 根据定理5.1.1的推论, 模p简化剩余系中每个元素的指数是$p-1$的因数, 所以有

$$\sum_{d\mid p-1}F(d)=p-1. \tag{5.25}$$

因为模p指数为d的元素满足同余式

$$x^d-1\equiv 0\ (\mathrm{mod}\ p), \tag{5.26}$$

根据定理3.4.5的推论, 同余式(5.26)有d个模p不同的解.

现在, 若a是模p指数为d的元素, 则同余式(5.26)的解可以表示成

$$x \equiv a^0,\ a,\ \cdots,\ a^{d-1}.$$

根据定理5.1.4, 这些数中有$\varphi(d)$个指数为d的元素. 因此, $F(d)=\varphi(d)$,而若没有模p指数为d的元素, 则$F(d)=0$. 总之, 有

$$F(d) \leqslant \varphi(d).$$

但由定理2.3.9, 又有

$$\sum_{d|p-1} \varphi(d) = p-1. \tag{5.27}$$

这样, 由式(5.25)和式(5.27)推出

$$\sum_{d|p-1} (\varphi(d) - F(d)) = 0. \tag{5.28}$$

因此, 对所有正整数$d \mid p-1$, 有

$$F(d) = \varphi(d). \tag{5.29}$$

特别地, 有

$$F(p-1) = \varphi(p-1).$$

这说明存在模p指数为$p-1$的元素, 即模p的原根存在. 证毕.

推论 设p是奇素数, d是$p-1$的正因数. 则模p 指数为d的元素存在.

证 从定理5.2.1证明的关系式(5.29), 即可推出结论. 证毕.

再给出原根的构造方法:

定理 5.2.2 *设p为奇素数, $p-1$的所有不同素因数是$q_1,\ \cdots,\ q_s$, 则g是模p原根的充要条件是*

$$g^{\frac{p-1}{q_i}} \not\equiv 1 \pmod{p}, \qquad i = 1, \cdots, s. \tag{5.30}$$

证 设g是p的一个原根, 则g对模p的指数是 $p-1$. 但

$$0 < \frac{p-1}{q_i} < p-1, \qquad i = 1, \cdots, s.$$

根据定理5.1.2, 有式 (5.30), 即

$$g^{\frac{p-1}{q_i}} \not\equiv 1 \pmod{p}, \qquad i = 1, \cdots, s.$$

反过来, 若g满足式(5.30), 但对模p的指数$e = \mathrm{ord}_p(g) < p-1$. 则根据定理5.1.1, 有$e \mid p-1$. 因而存在一个素数$q$使得$q \mid \dfrac{p-1}{e}$,即

$$\frac{p-1}{e} = u \cdot q \quad \text{或} \quad \frac{p-1}{q} = u \cdot e.$$

进而

$$g^{\frac{p-1}{q}} = (g^e)^u \equiv 1 \pmod{p}.$$

与假设式(5.30)矛盾. 证毕.

定理5.2.2给出了一个找原根的方法.

例 5.2.1 *求模$p=41$的所有原根.*

解　因为$p-1=40=2^3\cdot 5$, 其素因数为$q_1=2,\ q_2=5$. 进而, $\dfrac{p-1}{q_1}=20,\quad \dfrac{p-1}{q_2}=8$. 根据定理5.2.2, 只需要验证式(5.30), 即g^{20}、g^8模p是否同余于1. 对$g=2,\ 3,\ 5,\ 6$等, 逐个验算.

$$\begin{aligned}
&2^2\equiv 4, \quad 2^4\equiv 16, \quad 2^8\equiv 10, \quad 2^{16}\equiv 18, \quad 2^{20}\equiv 1,\\
&3^2\equiv 9, \quad 3^4\equiv -1, \quad 3^8\equiv 1, \quad 3^{16}\equiv 1, \quad 3^{20}\equiv -1,\\
&5^2\equiv 25, \quad 5^4\equiv 10, \quad 5^8\equiv 18, \quad 5^{16}\equiv 37, \quad 5^{20}\equiv 1,\\
&6^2\equiv 36, \quad 6^4\equiv 25, \quad 6^8\equiv 10, \quad 6^{16}\equiv 18, \quad 6^{20}\equiv -1 \pmod{41},
\end{aligned}$$

故$g=6$是模$p=41$的原根.

进一步, 当$(d,p-1)=1$时, d遍历模$p-1=40$的简化剩余系:

$$1,\ 3,\ 7,\ 9,\ 11,\ 13,\ 17,\ 19,\ 21,\ 23,\ 27,\ 29,\ 31,\ 33,\ 37,\ 39$$

共$\varphi(p-1)=16$个数时, g^d遍历模41的所有原根.

$$\begin{aligned}
&g^1\equiv 6, \quad g^3\equiv 11, \quad g^7\equiv 29, \quad g^9\equiv 19, \quad g^{11}\equiv 28, \quad g^{13}\equiv 24,\\
&g^{17}\equiv 26, \quad g^{19}\equiv 34, \quad g^{21}\equiv 35, \quad g^{23}\equiv 30, \quad g^{27}\equiv 12, \quad g^{29}\equiv 22,\\
&g^{31}\equiv 13, \quad g^{33}\equiv 17, \quad g^{37}\equiv 15, \quad g^{39}\equiv 7 \pmod{41}.
\end{aligned}$$

例 5.2.2　求模$p=43$的原根.

解　因为$p-1=42=2\cdot 3\cdot 7,\quad q_1=2,\ q_2=3,\ q_3=7$, 因此, $\dfrac{p-1}{q_1}=21,\quad \dfrac{p-1}{q_2}=14,\dfrac{p-1}{q_3}=6$. 只需要验证式(5.30), 即$g^{21}$、$g^{14}$、$g^6$模$p$是否同余于1. 对$g=2,\ 3,\ 5$等, 逐个验算.

$$\begin{aligned}
&2^2\equiv 4, \quad 2^4\equiv 16, \quad 2^6\equiv 64\equiv 21, \quad 2^7\equiv 21\cdot 2\equiv -1,\\
&2^{14}\equiv 1, \quad 3^2\equiv 9, \quad 3^4\equiv 81\equiv -5, \quad 3^6\equiv 9\cdot(-5)\equiv -2,\\
&3^7\equiv -6, \quad 3^{14}\equiv (-6)^2\equiv 36, \quad 3^{21}\equiv (-6)\cdot 36\equiv -1 \pmod{43}.
\end{aligned}$$

因此, $g=3$是模$p=43$的原根.

进一步, 当$(d,p-1)=1$时, d遍历模$p-1=42$的简化剩余系:

$$1,\ 5,\ 11,\ 13,\ 17,\ 19,\ 23,\ 25,\ 29,\ 31,\ 37,\ 41$$

共$\varphi(p-1)=12$个数时, g^d遍历模43的所有原根.

$$\begin{aligned}
&g^1\equiv 3, \quad g^5\equiv 28, \quad g^{11}\equiv 30, \quad g^{13}\equiv 12, \quad g^{17}\equiv 26, \quad g^{19}\equiv 19, \quad g^{23}\equiv 34,\\
&g^{25}\equiv 5, \quad g^{29}\equiv 18, \quad g^{31}\equiv 33, \quad g^{37}\equiv 20, \quad g^{41}\equiv 29 \pmod{43}.
\end{aligned}$$

例 5.2.3　求模$p=191$的原根.

解　因为$p-1=190=2\cdot 5\cdot 19,\ q_1=2,\ q_2=5,\ q_3=19$, 因此, $\dfrac{p-1}{q_1}=95,\ \dfrac{p-1}{q_2}=38,\ \dfrac{p-1}{q_3}=10$. 只需验证式(5.30), 即$g^{\frac{p-1}{q_1}}$、$g^{\frac{p-1}{q_2}}$、$g^{\frac{p-1}{q_3}}$模$p$是否同余于1. 对$g=2,\ 3,\ 5$等, 逐个验算.

g	$g^{\frac{p-1}{q_1}}$	$g^{\frac{p-1}{q_2}}$	$g^{\frac{p-1}{q_3}}$	g	$g^{\frac{p-1}{q_1}}$	$g^{\frac{p-1}{q_2}}$	$g^{\frac{p-1}{q_3}}$	g	$g^{\frac{p-1}{q_1}}$	$g^{\frac{p-1}{q_2}}$	$g^{\frac{p-1}{q_3}}$
2	1	49	69	10	1	49	180	15	1	39	153
3	1	39	30	11	190	1	107	17	1	109	32
5	1	1	177	12	1	49	153	18	1	39	25
6	1	1	160	13	1	184	121	19	190	39	52
7	190	39	1	14	190	1	69				

因此, $g=19$ 是模 $p=191$ 的原根.

5.2.2 模 p^α 原根

本节讨论模 p^α 原根的存在性.

先给出以下的引理:

引理 5.2.1 设 p 是一个奇素数. 如果整数 g 是模 p 原根, 则有

$$g^{p-1}\not\equiv 1 \pmod{p^2} \quad 或 \quad (g+p)^{p-1}\not\equiv 1 \pmod{p^2}.$$

证 因为

$$\begin{aligned}(g+p)^{p-1} &= g^{p-1}+\binom{p-1}{1}\cdot g^{p-2}\cdot p+\binom{p-1}{2}\cdot g^{p-3}\cdot p^2+\cdots+p^{p-1}\\ &= g^{p-1}+(p-1)\cdot g^{p-2}\cdot p+A\cdot p^2,\end{aligned}$$

其中 A 为整数, 所以有

$$(g+p)^{p-1}-1\equiv (g^{p-1}-1)+(p-1)\cdot g^{p-2}\cdot p \pmod{p^2}.$$

因此, 结论成立. 证毕.

引理 5.2.2 设 p 是一个奇素数. 如果整数 g 满足

$$g^{p-1}=1+u_0\cdot p,\quad (u_0,p)=1 \tag{5.31}$$

则对任意整数 $k\geqslant 2$, 存在整数 u_{k-2} 使得

$$g^{p^{k-2}(p-1)}=1+u_{k-2}\cdot p^{k-1},\quad (u_{k-2},p)=1. \tag{5.32}$$

证 对 $k\geqslant 2$ 作数学归纳法, 来证明关系式 (5.32), 即

$$g^{p^{k-2}(p-1)}=1+u_{k-2}\cdot p^{k-1},\quad (u_{k-2},p)=1.$$

$k=2$ 时, 关系式 (5.32) 就是关系式 (5.31), 命题成立.

假设 $k-1$ 时, 命题成立, 即存在整数 u_{k-3} 使得

$$g^{p^{k-3}(p-1)}=1+u_{k-3}\cdot p^{k-2},\quad (u_{k-3},p)=1.$$

两端作 p 次方, 有

$$g^{p^{k-2}(p-1)} = \left(1+u_{k-3}\cdot p^{k-2}\right)^p$$

$$\begin{aligned} &= 1+\binom{p}{1}\left(u_{k-3}\cdot p^{k-2}\right)+\binom{p}{2}\left(u_{k-3}\cdot p^{k-2}\right)^2+\cdots+\left(u_{k-3}\cdot p^{k-2}\right)^p \\ &= 1+(u_{k-3}+A_{k-3}\cdot p)\cdot p^{k-1} \end{aligned} \tag{5.33}$$

其中 A_{k-3} 为整数. 取 $u_{k-2}=u_{k-3}+A_{k-3}\cdot p$, 有 $(u_{k-2},p)=(u_{k-3},p)=1$. 命题成立.

根据数学归纳法原理, 关系式(5.32)对所有整数 $k\geqslant 2$ 成立. 证毕.

引理 5.2.3　设 p 是一个奇素数. 设 $k\geqslant 2$. 如果模 p 原根 g 满足

$$g^{p^{k-2}(p-1)}=1+u_{k-2}\cdot p^{k-1},\quad (u_{k-2},p)=1. \tag{5.34}$$

则 g 也是模 p^k 原根.

证　令 $e_k=\mathrm{ord}_{p^k}(g)$, 则有

$$g^{e_k}\equiv 1\ (\mathrm{mod}\ p^k).$$

进而, $g^{e_k}\equiv 1\ (\mathrm{mod}\ p)$. 因为 g 是模 p 原根, 所以 $p-1\mid e_k$. 故 e_k 具有形式 $e_k=p^t(p-1)$. 下面确定 $t=k-1$.

一方面, 根据引理5.2.2之证明式(5.2.2), 由假设条件式(5.34), 可得到

$$g^{p^{k-1}(p-1)}=1+(u_{k-2}+A_{k-2}\cdot p)\cdot p^k,$$

其中 A_{k-2} 为整数, 从而 $e_k\mid p^{k-1}(p-1),\ \ t\leqslant k-1$.

另一方面, 仍由假设条件式(5.34), 知

$$g^{p^{k-2}(p-1)}\not\equiv 1\ (\mathrm{mod}\ p^k),$$

得到 $e_k\nmid p^{k-2}(p-1),\ \ t>k-2$.

故 $t=k-1$, $e_k=p^{k-1}(p-1)=\varphi(p^k)$. g 也是模 p^k 的原根. 证毕.

其次, 构造模 p^2 的原根.

定理 5.2.3　设 g 是模 p 的一个原根, 则 g 或者 $g+p$ 是模 p^2 的原根.

证　根据引理5.2.1, 有式(5.31),

$$g^{p-1}=1+u_0\cdot p,\quad (u_0,p)=1$$

或

$$(g+p)^{p-1}=1+u_0\cdot p,\quad (u_0,p)=1.$$

再由引理5.2.3, 前者推出 g 是模 p^2 的原根, 而后者推出 $g+p$ 是模 p^2 的原根. 证毕.

再次, 构造模 p^α 的原根.

定理 5.2.4　设 p 是一个奇素数, 则对任意正整数 α, 模 p^α 的原根存在. 更确切地说, 如果 g 是模 p^2 的一个原根, 则对任意正整数 α, g 是模 p^α 的原根.

证　根据定理5.2.1, 知模 p 原根存在, 再由定理5.2.3及其证明知道模 p^2 的原根 g 也存在, 且满足式(5.31), 即

$$g^{p-1}=1+u_0\cdot p.$$

根据引理5.2.2, 对任意整数 $\alpha\geqslant 2$, 存在整数 $u_{\alpha-2}$ 使得式 (5.32) 成立, 即

$$g^{p^{\alpha-2}(p-1)}=1+u_{\alpha-2}\cdot p^{\alpha-1},\quad (u_{\alpha-2},p)=1.$$

因此, 根据引理5.2.3, g 是模 p^α 原根. 证毕.

定理 5.2.5　设 $\alpha\geqslant 1$, g 是模 p^α 的一个原根, 则 g 与 $g+p^\alpha$ 中的奇数是模 $2p^\alpha$ 的一个原根.

证 (i) 设奇数a满足同余式

$$a^d \equiv 1 \pmod{p^\alpha},$$

又显然有

$$a^d \equiv 1 \pmod{2},$$

根据定理2.1.12,

$$a^d \equiv 1 \pmod{2p^\alpha}.$$

反之亦然.

(ii) 若g是奇数, 令$d = \varphi(p^\alpha)$,则

$$\varphi(2p^\alpha) = \varphi(p^\alpha) = d.$$

又当

$$g^d \equiv 1 \pmod{p^\alpha}, \quad g^r \not\equiv 1 \pmod{p^\alpha}, \qquad 0 < r < d$$

时, 有

$$g^d \equiv 1 \pmod{2p^\alpha}, \quad g^r \not\equiv 1 \pmod{2p^\alpha}, \qquad 0 < r < d.$$

故g是模$2p^\alpha$的一个原根.

(iii) 若g是偶数, 则$g + p^\alpha$是奇数, 类似(ii)可得结论. 证毕.

例 5.2.4 设$m = 41^2 = 1681$, 求模m的原根.

解 由例5.2.1, 有$g = 6$是模$p = 41$的原根. 作计算

$$g^{p-1} = 6^{40} \equiv 143 \equiv 1 + 3 \cdot 41, \quad (g+p)^{p-1} = 47^{40} \equiv 1518 \equiv 1 + 37 \cdot 41 \pmod{41^2}.$$

因此, $g = 6$和$g + p = 47$都是模$m = p^2$的原根.

根据定理5.2.5和定理5.2.6, $(d, \varphi(m)) = 1$时, $\mathrm{ord}_m\left(g^d\right) = \mathrm{ord}_m(g)$,因此, 当$d$遍历模$\varphi\left(41^2\right) = 1640$的简化剩余系时, 6^d遍历模41^2的所有原根.

例 5.2.5 设$m = 2 \cdot 41^2 = 3362$, 求模m的原根.

解 这里应用定理5.2.4及例5.2.4, 即可得到$6 + 41^2 = 1687$和47是模$2 \cdot 41^2 = 3362$的原根.

例 5.2.6 设$m = 43^2 = 1849$, 求模m的原根.

解 由例5.2.2, 有$g = 3$是模$p = 41$的原根. 作计算

$$g^{p-1} = 3^{40} \equiv 143 \equiv 1 + 3 \cdot 41, \quad (g+p)^{p-1} = 47^{40} \equiv 1518 \equiv 1 + 37 \cdot 41 \pmod{41^2}.$$

因此, $g = 6$和$g + p = 47$都是模$m = p^2$的原根, 也都是模$m = p^\alpha$的原根.

例 5.2.7 设$m = 43^2 = 1849$, 求模m的原根.

解 因为已知3是模$p = 43$的原根, 所以根据定理5.2.3, 可知3或者$3 + 43 = 46$是模$43^2 = 1849$的原根. 事实上, 有

$$g^{p-1} = 3^{42} \equiv 87 \equiv 1 + 43 \cdot 2 \pmod{43^2}, \quad (g+p)^{p-1} = 46^{40} \equiv 689 \equiv 1 + 43 \cdot 16 \pmod{43^2}.$$

因此, $g = 3$和$g + p = 46$都是模$m = p^2$的原根, 也都是模$m = p^\alpha$的原根.

5.2.3 模2^α指数

先给出两个引理:

引理 5.2.4 设a是一个奇整数. 如果

$$a^2 = 1 + u_1 \cdot 2^t, \quad (u_1, 2) = 1,\ t \geqslant 3, \tag{5.35}$$

则对任意整数$k > t$, 存在整数u_{k-t}使得

$$a^{2^{k-t}} = 1 + u_{k-t} \cdot 2^{k-1}, \quad (u_{k-t}, 2) = 1. \tag{5.36}$$

证 对$k > t$作数学归纳法, 来证明关系式(5.36), 即

$$a^{2^{k-t}} = 1 + u_{k-t} \cdot 2^{k-1}, \quad (u_{k-t}, 2) = 1.$$

$k = t + 1$时, 关系式(5.36)就是关系式(5.35), 命题成立.

假设$k - 1 > t$时, 命题成立, 即存在整数u_{k-1-t}使得

$$a^{2^{k-1-t}} = 1 + u_{k-1-t} \cdot 2^{k-2}, \quad (u_{k-1-t}, 2) = 1.$$

两端作二次方, 有

$$a^{2^{k-t}} = 1 + \left(u_{k-1-t} + u_{k-1-t}^2 \cdot 2^{k-3}\right) \cdot 2^{k-1} = 1 + u_{k-t} \cdot 2^{k-1} \tag{5.37}$$

其中$u_{k-t} = u_{k-1-t} + u_{k-1-t}^2 \cdot 2^{k-3}$满足$(u_{k-t}, 2) = (u_{k-1-t}, 2) = 1$. 命题成立.

引理 5.2.5 设整数$t \geqslant 3$. 对于整数$k > t$, 如果奇整数a满足关系式(5.36), 即

$$a^{2^{k-t}} = 1 + u_{k-t} \cdot 2^{k-1}, \quad (u_{k-t}, 2) = 1,$$

则 a模2^k的指数为2^{k-t+1}.

证 令$e_k = \mathrm{ord}_{2^k}(a)$. 则有

$$a^{e_k} \equiv 1 \pmod{2^k}.$$

根据欧拉定理(定理2.4.1), 有$e_k \mid \varphi(2^k) = 2^{k-1}$. 所以 e_k具有形式$e_k = 2^s$. 下面确定 $s = k - t + 1$.

一方面, 根据引理5.2.4证明式(5.38), 由假设条件式(5.36), 可得到

$$a^{2^{k-t+1}} = 1 + \left(u_{k-t} + u_{k-t}^2 \cdot 2^{k-2}\right) \cdot 2^k = 1 + u_{k-t+1} \cdot 2^k, \tag{5.38}$$

其中$u_{k-t+1} = u_{k-t} + u_{k-t}^2 \cdot 2^{k-2}$满足$(u_{k-t+1}, 2) = (u_{k-t}, 2) = 1$, 从而$e_k \mid 2^{k-t+1}$, $s \leqslant k - t + 1$.

另一方面, 仍由假设条件式(5.36), 知

$$a^{2^{k-t}} \not\equiv 1 \pmod{2^k},$$

得到$e_k \nmid 2^{k-t}$, $s > k - t$.

故$s = k - t + 1$, $e_k = 2^{k-t+1} = \varphi(p^k)/2^{t-2}$. 证毕.

再讨论奇整数的指数的上界.

定理 5.2.6 设a是一个奇整数. 则对任意整数$\alpha \geqslant 3$, 有a模2^α的指数不大于$\varphi(2^\alpha)/2 = 2^{\alpha-2}$, 即

$$a^{\varphi(2^\alpha)/2} \equiv a^{2^{\alpha-2}} \equiv 1 \pmod{2^\alpha}. \tag{5.39}$$

证 将奇整数a写成$a = 1 + b \cdot 2$, 因为$2 \mid b(b+1)$, 所以有

$$a^2 = 1 + b(b+1) \cdot 2^2 = 1 + u_1 \cdot 2^t, \quad (u_1, 2) = 1,\ t \geqslant 3.$$

对于整数$\alpha \geqslant 3$, 当$\alpha \leqslant t$时, 有

$$a^2 \equiv 1 \pmod{2^\alpha},$$

所以 a 模2^α 的指数为$2 \leqslant \varphi(2^\alpha)/2 = 2^{\alpha-2}$.

而当$\alpha > t$时, 由引理5.2.4, 知有关系式

$$a^{2^{\alpha-t}} = 1 + u_{\alpha-t} \cdot 2^{\alpha-1}, \quad (u_{\alpha-t}, 2) = 1,$$

成立. 因此, 根据引理5.2.5, a 模2^α 的指数为 $2^{\alpha-t+1} \leqslant \varphi(2^\alpha)/2 = 2^{\alpha-2}$. 证毕.

定理 5.2.7 设$\alpha \geqslant 3$是一个整数, 则

$$\mathrm{ord}_{2^\alpha}(5) = \varphi(2^\alpha)/2 = 2^{\alpha-2}.$$

证 因为$a = 5$具有形式

$$a^2 = 1 + 3 \cdot 2^3 = 1 + u_1 \cdot 2^t, \quad u_1 = 3,\ t = 3,$$

对于整数$\alpha \geqslant 3$, 由引理5.2.4知有关系式

$$a^{2^{\alpha-t}} = 1 + u_{\alpha-t} \cdot 2^{\alpha-1}, \quad (u_{\alpha-t}, 2) = 1,$$

成立. 因此, 根据引理5.2.5, $a = 5$模2^α 的指数为 $2^{\alpha-t+1} = \varphi(2^\alpha)/2$. 证毕.

例 5.2.8 设$\alpha \geqslant 3$是一个整数, 则对于整数 $a = 8k + 3$,

$$\mathrm{ord}_{2^\alpha}(a) = \varphi(2^\alpha)/2.$$

证 因为$a = 8k + 3$具有形式

$$a^2 = 1 + \left[1 + 2(3k + 4k^2)\right] \cdot 2^3 = 1 + u_1 \cdot 2^t, \quad u_1 = 1 + 2(3k + 4k^2),\ t = 3,$$

对于整数$\alpha \geqslant 3$, 由引理5.2.4有关系式

$$a^{2^{\alpha-t}} = 1 + u_{\alpha-t} \cdot 2^{\alpha-1}, \quad (u_{\alpha-t}, 2) = 1,$$

成立. 因此, 根据引理5.2.5, $a = 8k + 3$模2^α 的指数为$2^{\alpha-t+1} = \varphi(2^\alpha)/2$. 证毕.

例 5.2.9 设$\alpha \geqslant 3$是一个整数, 则对于整数$a = 2^s - 1$, $3 \leqslant s < \alpha$, 有

$$\mathrm{ord}_{2^\alpha}(a) = 2^{\alpha-s}.$$

证 因为$a = 2^s - 1$具有形式

$$a^2 = 2^{2s} - 2^{s+1} + 1 = 1 + (2^{s-1} - 1) \cdot 2^{s+1} = 1 + u_1 \cdot 2^t, \quad u_1 = 2^{s-1} - 1,\ t = s + 1,$$

对于整数$\alpha \geqslant 3$, 由引理5.2.4有关系式

$$a^{2^{\alpha-t}} = 1 + u_{\alpha-t} \cdot 2^{\alpha-1}, \quad (u_{\alpha-t}, 2) = 1,$$

成立. 因此, 根据引理5.2.5, $a = 2^s - 1$模2^α 的指数为$2^{\alpha-t+1} = 2^{\alpha-s}$. 证毕.

5.2.4 模m原根

本节给出模m原根存在的充要条件.

定理 5.2.8 模m的原根存在的充要条件是 $m = 2$, 4, p^α, $2p^\alpha$, 其中p是奇素数.

证　必要性. 设m的标准分解式为

$$m=2^{\alpha}p_1^{\alpha_1}\cdots 2p_k^{\alpha_k}.$$

若$(a,m)=1$,则

$$(a,2^{\alpha})=1,\quad (a,p_i^{\alpha_i})=1,\quad i=1,\cdots,k.$$

根据定理2.4.1(欧拉定理)及定理5.2.6, 有

$$\begin{cases} a^{\tau} & \equiv 1 \pmod{2^{\alpha}},\\ a^{\varphi(p_1^{\alpha_1})} & \equiv 1 \pmod{p_1^{\alpha_1}},\\ & \vdots\\ a^{\varphi(p_k^{\alpha_k})} & \equiv 1 \pmod{p_k^{\alpha_k}}, \end{cases}$$

其中$\tau=\begin{cases} \varphi(2^{\alpha}), & \alpha\leqslant 2,\\ \dfrac{1}{2}\varphi(2^{\alpha}), & \alpha\geqslant 3. \end{cases}$

令

$$h=[\tau,\ \varphi(p_1^{\alpha_1}),\ \cdots,\ \varphi(p_k^{\alpha_k})].$$

根据定理5.1.6之推论, 对所有整数a, $(a,m)=1$,有

$$a^h\equiv 1 \pmod{m}.$$

因此, 若$h<\varphi(m)$, 则模m的原根不存在.

现在讨论何时

$$h=\varphi(m)=\varphi(2^{\alpha})\varphi(p_1^{\alpha_1})\cdots\varphi(p_k^{\alpha_k}).$$

(1) 当$\alpha\geqslant 3$时, $\tau=\dfrac{\varphi(2^{\alpha})}{2}$. 因此,

$$h\leqslant\frac{\varphi(m)}{2}<\varphi(m).$$

(2) 当$k\geqslant 2$时, $2\mid\varphi(p_1^{\alpha_1}),\quad 2\mid\varphi(p_2^{\alpha_2})$. 进而,

$$[\varphi(p_1^{\alpha_1}),\varphi(p_2^{\alpha_2})]\leqslant\frac{1}{2}\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})<\varphi(p_1^{\alpha_1}p_2^{\alpha_2}).$$

因此, $h<\varphi(m)$.

(3) 当$\alpha=2$, $k=1$时,

$$\varphi(2^{\alpha})=2,\quad 2\mid\varphi(p_1^{\alpha_1}).$$

因此,

$$h=\varphi(p_1^{\alpha_1})<\varphi(2^n)\varphi(p_1^{\alpha_1})=\varphi(m).$$

故只有在(α,k)是

$$(1,0),\ (2,0),\ (0,1),\ (1,1)$$

4种情形之一, 即只有在m是

$$2,\ 4,\ p^{\alpha},\ 2p^{\alpha}$$

4个数之一时, 才有可能使$h=\varphi(m)$. 因此必要性成立.

充分性. 当$m=2$时, $\varphi(2)=1$, 整数1是模2的原根;

当$m=4$时, $\varphi(4)=2$, 整数3是模4的原根;
当$m=p^{\alpha}$时, 根据定理5.2.4, 模m的原根存在;
当$m=2p^{\alpha}$时, 根据定理5.2.5, 模m的原根存在.
因此, 条件的充分性是成立的. 证毕.

例 5.2.10 设$m=41$, 求模m的所有整数的指数表.

解 模$m=41$的指数表为

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

例 5.2.11 设$m=43$, 求模m的所有整数的指数表.

解 模$m=43$的指数表为

a	order	a	order	a	order	a	order	a	order
1	1	11	7	21	7	31	21	41	7
2	14	12	42	22	14	32	14	42	2
3	42	13	21	23	21	33	42		
4	7	14	21	24	21	34	42		
5	42	15	21	25	21	35	7		
6	3	16	7	26	42	36	3		
7	6	17	21	27	14	37	6		
8	14	18	42	28	42	38	21		
9	21	19	42	29	42	39	14		
10	21	20	42	30	42	40	21		

例 5.2.12 设$m=167$, 求模m的所有整数的指数表.

解 模$m=167$的指数表为

a	order	a	order	a	order	a	order	a	order
1	1	8	83	15	166	22	83	29	83
2	83	9	83	16	83	23	166	30	166
3	83	10	166	17	166	24	83	31	83
4	83	11	83	18	83	25	83	32	83
5	166	12	83	19	83	26	166	33	83
6	83	13	166	20	166	27	83	34	166
7	83	14	83	21	83	28	83	35	166

续表

a	order	a	order	a	order	a	order	a	order
36	83	63	83	90	166	117	166	144	83
37	166	64	83	91	166	118	166	145	166
38	83	65	83	92	166	119	166	146	166
39	166	66	83	93	83	120	166	147	83
40	166	67	166	94	83	121	83	148	166
41	166	68	166	95	166	122	83	149	166
42	83	69	166	96	83	123	166	150	83
43	166	70	166	97	83	124	83	151	166
44	83	71	166	98	83	125	166	152	83
45	166	72	83	99	83	126	83	153	166
46	166	73	166	100	83	127	83	154	83
47	83	74	166	101	166	128	83	155	166
48	83	75	83	102	166	129	166	156	166
49	83	76	83	103	166	130	83	157	83
50	83	77	83	104	166	131	166	158	166
51	166	78	166	105	166	132	83	159	166
52	166	79	166	106	166	133	83	160	166
53	166	80	166	107	83	134	166	161	166
54	83	81	83	108	83	135	166	162	83
55	166	82	166	109	166	136	166	163	166
56	83	83	166	110	166	137	83	164	166
57	83	84	83	111	166	138	166	165	166
58	83	85	83	112	83	139	166	166	2
59	166	86	166	113	166	140	166		
60	166	87	83	114	83	141	83		
61	83	88	83	115	83	142	166		
62	83	89	83	116	83	143	166		

例 5.2.13　求模 $m = 53$ 的原根.

解　设 $m = 53$, 则

$$\varphi(m) = \varphi(53) = 2^2 \cdot 13, \quad q_1 = 2,\ q_2 = 13.$$

因此,

$$\varphi(m)/q_1 = 26, \quad \varphi(m)/q_2 = 4.$$

这样, 只需验证：g^{26}、g^4 模 m 是否同余于 1. 对 2、3 等逐个验算.

$$2^2 \equiv 4, \quad 2^4 \equiv 16, \quad 2^8 \equiv 44, \quad 2^{12} \equiv 15,$$

$$2^{13} \equiv 30, \quad 2^{26} \equiv 52 \equiv -1 \pmod{53}.$$

因此, $g = 2$ 是模 $m = 53$ 的原根.

例 5.2.14　求模 $m = 109$ 的原根.

解 设$m=109$, 则

$$\varphi(m)=\varphi(109)=108=2^2\cdot 3^3,\quad q_1=2,\ q_2=3.$$

因此,

$$\varphi(m)/q_1=54,\quad \varphi(m)/q_2=36.$$

这样, 只需验证: g^{54}、g^{36}模m是否同余于1. 对2、3、5、6等逐个验算.

$$2^{54}\equiv 108,\quad 2^{36}\equiv 1,\quad 3^{54}\equiv 1,\quad 3^{36}\equiv 63,$$

$$5^{54}\equiv 1,\quad 5^{36}\equiv 63,\quad 6^{54}\equiv 108,\quad 6^{36}\equiv 63\ (\mathrm{mod}\ 109).$$

因此, $g=6$是模$m=109$的原根.

例 5.2.15 *求模$m=113$的原根.*

解 设$m=113$, 则

$$\varphi(m)=\varphi(113)=112=2^4\cdot 7,\quad q_1=2,\ q_2=7.$$

因此,

$$\varphi(m)/q_1=56,\quad \varphi(m)/q_2=16.$$

这样, 只需验证: g^{56}、g^{16}模m是否同余于1. 对2、3、5、6等逐个验算.

$$2^{56}\equiv 1,\quad 2^{16}\equiv 109,\quad 3^{56}\equiv 112,\quad 3^{36}\equiv 49\ (\mathrm{mod}\ 113).$$

因此, $g=3$是模$m=113$的原根.

例 5.2.16 *求模$m=59$的原根.*

解 设$m=59$, 则

$$\varphi(m)=\varphi(59)=2\cdot 29,\quad q_1=2,\ q_2=29.$$

因此,

$$\varphi(m)/q_1=29,\quad \varphi(m)/q_2=2.$$

这样, 只需验证: g^{29}、g^2模m是否同余于1. 对2、3等逐个验算.

$$2^2\equiv 4,\quad 2^{29}\equiv 58\equiv -1\pmod{59}.$$

因此, $g=2$是模$m=59$的原根.

例 5.2.17 *求模$m=61$的原根.*

解 设$m=61$, 则

$$\varphi(m)=\varphi(61)=2^2\cdot 3\cdot 5,\quad q_1=2,\ q_2=29,\ q_3=5.$$

因此,

$$\varphi(m)/q_1=30,\quad \varphi(m)/q_2=20,\quad \varphi(m)/q_3=12.$$

这样, 只需验证：g^{30}、g^{20}、g^{12}模m是否同余于1. 对2、3等逐个验算.

$$2^{30}\equiv 60,\quad 2^{20}\equiv 47,\quad 2^{12}\equiv 9\pmod{61}.$$

因此, $g=2$是模$m=61$的原根.

5.3 指标及n次同余式

5.3.1 指标

在$m=p^{\alpha}$或$2p^{\alpha}$的情形下, 模m的原根g是存在的.

利用原根引进指标的概念, 并应用指标的性质来研究同余式

$$x^n \equiv a \pmod{m}, \qquad (a,m)=1 \tag{5.40}$$

有解的条件及解数.

根据定理5.1.2, 知道: 当r遍历模$\varphi(m)$的最小正完全剩余系时, g^r遍历模m的一个简化剩余系. 因此, 对任意的整数a, $(a,m)=1$, 存在唯一的整数r, $1\leqslant r\leqslant \varphi(m)$, 使得

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

定义 5.3.1 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, 则存在唯一的整数r使得

$$g^r \equiv a \pmod{m}, \quad 1\leqslant r\leqslant \varphi(m) \tag{5.41}$$

成立, 这个整数r叫作以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 5.3.1 整数5是模17的原根, 并且有

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	16	12	9	11	4	3	15	7	1

因此, 有

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

定理 5.3.1 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. 如果整数r使得同余式

$$g^r \equiv a \pmod{m} \tag{5.42}$$

成立, 则这个整数r满足

$$r \equiv \mathrm{ind}_g a \pmod{\varphi(m)}. \tag{5.43}$$

证 因为$(a,m)=1$, 所以有

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

从而,

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

又因为g模m的指数是$\varphi(m)$, 根据定理5.1.1

$$\varphi(m) \mid r-\mathrm{ind}_g a.$$

因此, 式(5.43)成立. 证毕.

推论 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

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

证 因为

$$g^0 \equiv 1 \pmod{m},$$

根据定理5.3.1, 有

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

定理 5.3.2 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$1 \leqslant r \leqslant \varphi(m)$, 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, 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. 证毕.

定理 5.3.3 设m是大于 1 的整数, g是模m的一个原根. 若$a_1, \cdots, a_n$是与m互素的n个整数, 则

$$\mathrm{ind}_g(a_1 \cdots a_n) \equiv \mathrm{ind}_g(a_1) + \cdots + \mathrm{ind}_g(a_n) \pmod{\varphi(m)}. \tag{5.44}$$

特别地,

$$\mathrm{ind}_g(a^n) \equiv n\ \mathrm{ind}_g(a) \pmod{\varphi(m)}. \tag{5.45}$$

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

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

从而

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

根据定理5.3.1, 得到式 (5.44), 即

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

特别地, 对于$a_1 = \cdots = a_n = a$, 有式(5.45) 成立. 证毕.

例 5.3.2 作模41的指标表.

解 已知6是模41的原根, 直接计算$g^r \pmod{m}$.

$$\begin{array}{llllll}
6^{40} \equiv 1, & 6^1 \equiv 6, & 6^2 \equiv 19, & 6^3 \equiv 11, & 6^4 \equiv 25, & 6^5 \equiv 27, \\
6^6 \equiv 39, & 6^7 \equiv 29, & 6^8 \equiv 10, & 6^9 \equiv 19, & 6^{10} \equiv 32, & 6^{11} \equiv 28, \\
6^{12} \equiv 4, & 6^{13} \equiv 24, & 6^{14} \equiv 21, & 6^{15} \equiv 3, & 6^{16} \equiv 18, & 6^{17} \equiv 26, \\
6^{18} \equiv 33, & 6^{19} \equiv 34, & 6^{20} \equiv 40, & 6^{21} \equiv 35, & 6^{22} \equiv 5, & 6^{23} \equiv 30, \\
6^{24} \equiv 16, & 6^{25} \equiv 14, & 6^{26} \equiv 2, & 6^{27} \equiv 12, & 6^{28} \equiv 31, & 6^{29} \equiv 22, \\
6^{30} \equiv 9, & 6^{31} \equiv 13, & 6^{32} \equiv 37, & 6^{33} \equiv 17, & 6^{34} \equiv 20, & 6^{35} \equiv 38, \\
6^{36} \equiv 23, & 6^{37} \equiv 15, & 6^{38} \equiv 8, & 6^{39} \equiv 7 & \pmod{41}. &
\end{array}$$

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的数.

	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									

例 5.3.3 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 所在的行, 个位数 8 所在的列, 交叉位置的数 11 就是 $\mathrm{ind}_6 28=11$. 而查找十位数 1 所在的行, 个位数 8 所在的列, 交叉位置的数 16 就是 $\mathrm{ind}_6 18=16$.

5.3.2 n 次同余式

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 5.3.2 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

$$x^n \equiv a \pmod m \tag{5.46}$$

有解, 则 a 叫作对模 m 的 n **次剩余**; 否则, a 叫作对模 m 的 n **次非剩余**.

例 5.3.4 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 $x \equiv 6^y \pmod{41}$, 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5.3.1, 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

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

定理 5.3.4 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, 则同余式 (5.46)

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

有解的充分必要条件是

$$(n, \varphi(m)) \mid \mathrm{ind} a, \tag{5.47}$$

且在有解的情况下, 解数为 $(n,\varphi(m))$.

证 若同余式(5.46) 有解

$$x \equiv x_0 \pmod{m},$$

则分别存在非负整数 u、r 使得

$$x_0 \equiv g^u, \quad a \equiv g^r \pmod{m}.$$

由式(5.46)得

$$g^{u\,n} \equiv g^r \pmod{m}$$

或

$$u\,n \equiv r \pmod{\varphi(m)}.$$

即同余式

$$n\,X \equiv r \pmod{\varphi(m)} \tag{5.48}$$

有解 $X \equiv u \pmod{\varphi(m)}$. 因此, 式(5.47) 成立.

反过来, 若式 (5.47) 成立, 则式 (5.48) 有解

$$X \equiv u \pmod{\varphi(m)},$$

且解数为 $(n,\varphi(m))$. 因此, 式(5.46) 有解

$$x_0 \equiv g^u \pmod{m},$$

解数为 $(n,\varphi(m))$. 证毕.

推论 在定理5.3.4的假设条件下, a 是模 m 的 n 次剩余的充分必要条件是

$$a^{\frac{\varphi(m)}{d}} \equiv 1 \pmod{m}, \qquad d=(n,\varphi(m)). \tag{5.49}$$

证 由定理5.3.4证明: 同余式 (5.46)

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

有解的充分必要条件是同余式 (5.48)

$$n\,X \equiv r \pmod{\varphi(m)}$$

有解. 而这等价于式 (5.47)

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

即

$$\mathrm{ind}a \equiv 0 \pmod{d}.$$

两端同乘以 $\dfrac{\varphi(m)}{d}$, 得到

$$\frac{\varphi(m)}{d}\mathrm{ind}a \equiv 0 \pmod{\varphi(m)}.$$

这等价于式 (5.49). 证毕.

例 5.3.5 求解同余式

$$x^8 \equiv 23 \pmod{41}.$$

解 因为

$$d=(n,\varphi(m))=(8,\varphi(41))=(8,40)=8,$$

$$\mathrm{ind}23=36.$$

又 36 不能被 8 整除, 所以由定理5.3.4得同余式无解.

例 5.3.6 *求解同余式*

$$x^{12}\equiv 37\ (\mathrm{mod}\ 41).$$

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

$$12\ \mathrm{ind}x\equiv \mathrm{ind}37\ (\mathrm{mod}\ 40)$$

或

$$3\ \mathrm{ind}x\equiv 8\ (\mathrm{mod}\ 10).$$

得到

$$\mathrm{ind}x\equiv 6,\ 16,\ 26,\ 36\ (\mathrm{mod}\ 40).$$

查指标表得原同余式解

$$x\equiv 39,\ 18,\ 2,\ 23\ (\mathrm{mod}\ 41).$$

定理 5.3.5 *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 a 对模 m 的指数是*

$$e=\frac{\varphi(m)}{(\mathrm{ind}a,\varphi(m))}. \tag{5.50}$$

特别地, a 是模 m 的原根当且仅当

$$(\mathrm{ind}a,\varphi(m))=1. \tag{5.51}$$

证 因为模 m 有原根 g, 所以有

$$a=g^{\mathrm{ind}a}\ (\mathrm{mod}\ m).$$

根据定理5.1.3, a 的指数为

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

显然, a 是模 m 的原根的充分必要条件是 $\mathrm{ord}(a)=\varphi(m)$, 即式 (5.51) 成立. 证毕.

定理 5.3.6 *设 m 是大于 1 的整数, 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, 根据定理5.1.3, 知 $a=g^d$ 的指数为

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

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 $d = d'\dfrac{\varphi(m)}{e}$，$0 \leqslant d' < e$. 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 $\varphi(\varphi(m))$. 证毕.

5.4 习　　题

扫一扫 习题

扫一扫 自测题