第 4 章　阶与原根

本章将进一步讨论同余方程 $x^n \equiv a(\bmod m), (a,m)=1$ 中指数与底数的关系. 首先，引入阶和原根的概念，着重介绍阶的基本性质，以及由模素数 p 原根的存在性延申至一般情形下模 m 原根的存在性，并给出求原根的构造性方法. 再由原根引入指标的概念，并揭示同余方程 $x^n \equiv a(\bmod m), (a,m)=1$ 有解的条件及解数. 由此可以看到，阶与原根是数论中的基本概念，也是解决特定类型同余方程的有力工具. 同时，它们在密码学中也有着重要的应用，如离散对数问题，是许多密码算法和协议(如 Diffie-Hellman 密钥交换等)的理论基础。

因此，通过深入研究它们的性质和应用，我们可以进一步拓展数学视野，并探索更多数学与实际应用之间的桥梁.

本章的知识要点：

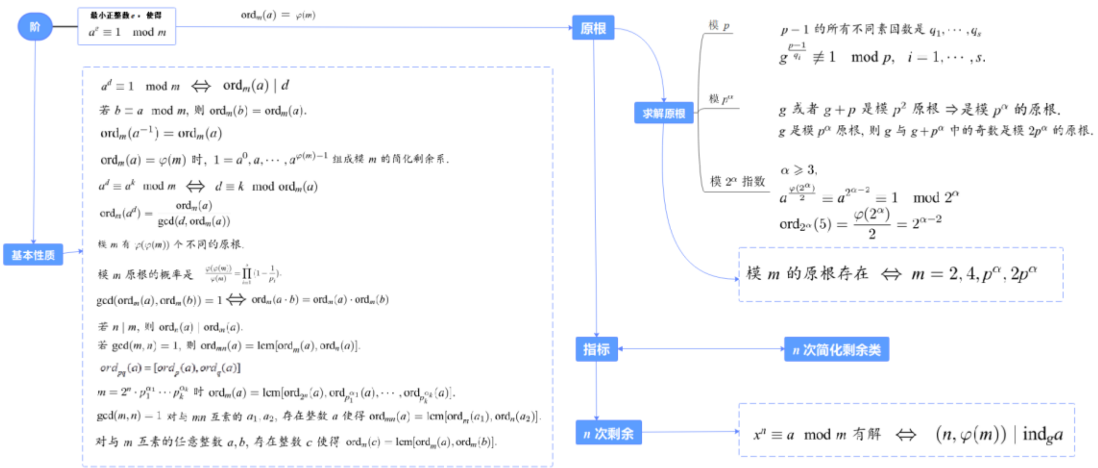

图 4-1 阶与原根知识点图谱

4.1 阶及其基本性质

设 $m>1$ 是整数，a 是与 m 互素的正整数，根据定理 2.2.13（欧拉定理），我们有

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

当然，我们要问该 $\varphi(m)$ 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？

4.1.1 阶与原根的定义

定义 4.1.1　设 $m>1$ 是整数，a 是与 m 互素的正整数，则使得

$$a^e \equiv 1 (\bmod m)$$

成立的最小正整数 e 叫做 a 对模 m 的**阶(或指数)**，记作 $ord_m(a)$. 如果 a 对模 m 的阶是 $\varphi(m)$，则 a 叫做模 m 的**原根**.

例 4.1.1 设整数 m=7，这时 $\varphi(7)=6$，我们有

$$\begin{array}{lll} 1^1 \equiv 1 & 2^3 = 8 \equiv 1 & 3^3 = 27 \equiv -1 \\ 4^3 = (-3)^3 \equiv 1 & 5^3 = (-2)^3 \equiv -1 & 6^2 = (-1)^2 \equiv 1 (\bmod 7) \end{array}.$$

列成表为：

a	1	2	3	4	5	6
$ord_m(a)$	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 4.1.2 设整数 m=14=2*7，这时 $\varphi(14)=6$，我们有

$$\begin{array}{lll} 1^1 \equiv 1 & 3^3 = 27 \equiv -1 & 5^3 = 125 \equiv -1 \\ 9^3 \equiv (-5)^3 \equiv 1 & 11^3 \equiv (-3)^3 \equiv 1 & 13^2 \equiv (-1)^2 \equiv 1 \quad (\bmod 14) \end{array}.$$

列成表为：

a	1	3	5	9	11	13
$ord_m(a)$	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 4.1.3 设整数 m=21=3*7，这时 $\varphi(21) = 12$，我们有

$$\begin{array}{lll} 1^1 \equiv 1 & 2^6 = 64 \equiv 1 & 4^3 = 64 \equiv 1 \\ 5^6 = 15625 \equiv 1 & 8^2 \equiv 1 & 10^6 = (2 \cdot 5)^6 \equiv 1 \\ 11^6 \equiv (-10)^6 \equiv 1 & 13^2 = (-8)^2 \equiv 1 & 16^6 \equiv (-5)^6 \equiv 1 \\ 17^6 \equiv (-4)^6 \equiv 1 & 19^6 \equiv (-2)^6 \equiv 1 & 20^2 \equiv (-1)^2 \equiv 1 \ (\bmod 21). \end{array}$$

列成表为：

a	1	2	4	5	8	10	11	13	16	17	19	20
$ord_m(a)$	1	6	3	6	2	6	6	2	6	6	6	2

因此，没有模 21 的原根.

例 4.1.4 设整数 m=9=3^2，这时 $\varphi(9)=6$，我们有

$$1^1\equiv 1 \qquad 2^3=8\equiv -1 \qquad 4^3=64\equiv 1$$
$$5^3=(-4)^3\equiv -1 \quad 7^3=(-2)^3\equiv 1 \quad 8^2=(-1)^2\equiv 1 \pmod 9.$$

列成表为：

a	1	2	4	5	7	8
$ord_m(a)$	1	6	3	6	3	2

因此，2, 5 是模 9 的原根.

例 4.1.5 设整数 m=8=2^3，这时 $\varphi(8)=4$，我们有

$$1^1\equiv 1 \qquad 3^2=9\equiv 1 \qquad 5^2=25\equiv 1 \qquad 7^2=(-1)^2\equiv 1 \pmod 8$$

列成表为

a	1	3	5	7
$ord_m(a)$	1	2	2	2

因此，没有模 8 的原根.

4.1.2 阶的基本性质

现在讨论阶的基本性质，类似于最小周期.

定理 4.1.1 设 m>1 是整数，a 是与 m 互素的整数，则整数 d 使得 $a^d\equiv 1 \pmod m$ 的充分必要条件是 $ord_m(a)|d$.

证 充分性：设 $ord_m(a)|d$，那么存在整数 k 使得 $d=k\,ord_m(a)$. 因此，我们有

$$a^d=\left(a^{ord_m(a)}\right)^k\equiv 1 \pmod m.$$

必要性：如果 $ord_m(a)|d$ 不成立，

则由定理 1.1.11（欧几里德除法），存在整数 q，r 使得

$$d = ord_m(a)q + r,\ 0 < r < ord_m(a).$$

从而，

$$a^r = a^r \left(a^{ord_m(a)}\right)^q = a^d \equiv 1(\bmod m).$$

这与$ord_m(a)$的最小性矛盾，故$ord_m(a)|d$.

推论 4.1.1 设 m>1 是整数，a 是与 m 互素的整数，则$ord_m(a)|\varphi(m)$.

证 根据定理 2.2.13（欧拉定理），我们有 $a^{\varphi(m)} \equiv 1(\bmod m)$.

由定理 4.1.1，我们有$ord_m(a)|\varphi(m)$.

根据推论 4.1.1，整数 a 模 m 的阶$ord_m(a)$是$\varphi(m)$的因数，所以我们可以在$\varphi(m)$的因数中求$ord_m(a)$.

例 4.1.6 求整数 2 模 13 的阶$ord_{13}(2)$.

解 因为$\varphi(13) = 12$，

所以我们只需对 12 的因数 d=1, 2, 3, 4, 6, 12，计算$2^d(mod\, m)$.

因为

$2^1 \equiv 2$， $2^2 \equiv 4$， $2^3 \equiv 8$， $2^4 \equiv 16 \equiv 3$，

$2^6 \equiv 64 \equiv -1$， $2^{12} \equiv (-1)^2 \equiv 1(mod\, 13)$，

所以 $ord_{13}(2) = 12$.

这也说明 2 是模 12 的原根.

推论 4.1.2 设 p 是奇素数，且$(p-1)/2$也是素数，如果 a 是一个不被 p 整除的整数，且也不是模 p 的二次单位根，则

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

证 根据定理 2.2.13（欧拉定理），有$a^{\varphi(p)} \equiv 1(\bmod p)$.

根据推论 4.1.1，整数 a 模 p 的阶$ord_p(a)$是$\varphi(p) = p-1 = 2\cdot\frac{p-1}{2}$的因数，

但$ord_p(a) \neq 2$，所以

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

推论 4.1.3 设 $m>1$ 是整数，a 是与 m 互素的整数.

(i) 若 $b \equiv a \pmod m$，则 $ord_m(b) = ord_m(a)$.

(ii) 设 a^{-1} 使得 $a^{-1}a \equiv 1 \pmod m$，则 $ord_m(a^{-1}) = ord_m(a)$.

证 (i) 若 $b \equiv a \pmod m$，则 $b^{ord_m(a)} \equiv a^{ord_m(a)} \equiv 1 \pmod m$.

因此，我们有 $ord_m(b) | ord_m(a)$.

同样，我们有 $ord_m(a) | ord_m(b)$.

故 $ord_m(b) = ord_m(a)$.

(ii) 因为 $(a^{-1})^{ord_m(a)} \equiv (a^{ord_m(a)})^{-1} \equiv 1 \pmod m$，

因此，我们有 $ord_m(a^{-1}) | ord_m(a)$.

同理 $ord_m(a) | ord_m(a^{-1})$.

故 $ord_m(a^{-1}) = ord_m(a)$.

例 4.1.7 整数 28 模 13 的阶为 $ord_{13}(28) = ord_{13}(2) = 12$.

整数 7 模 13 的阶为 12，因为 $2^{-1} \equiv 7 (mod\, 1\,3)$（由例 4.1.6 可知）.

定理 4.1.2 设 $m>1$ 是整数，a 是与 m 互素的整数，则

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

模 m 两两不同余. 特别地，当 a 是模 m 的原根，即 $ord_m(a) = \varphi(m)$ 时，这个 $\varphi(m)$ 个数

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

组成模 m 的简化剩余系.

证 反证法. 若存在整数 $0 \le k,\ \ l < ord_m(a)$ 使得 $a^k \equiv a^l \pmod m$.

不妨设 $k>l$，由于 $(a,m)=1$，得到 $a^{k-l} \equiv 1 \pmod m$.

但 $0 < k-l < ord_m(a)$，这与 $ord_m(a)$ 的最小性矛盾. 因此，结论成立.

再设 a 是模 m 的原根，即 $ord_m(a) = \varphi(m)$，

则我们有 $\varphi(m)$ 个数 $1 = a^0, a, \cdots, a^{\varphi(a)-1}$ 模 m 两两不同余.

根据定理 2.2.7，这 $\varphi(m)$ 个数组成模 m 的简化剩余系.

例 4.1.8 整数$\{2^k | k=0,\cdots,11\}$组成模 13 的简化剩余系.

$2^0 \equiv 1$， $2^1 \equiv 2$， $2^2 \equiv 4$，

$2^3 \equiv 8$， $2^4 = 16 \equiv 3$， $2^5 \equiv 3 \cdot 2 \equiv 6$，

$2^6 \equiv 6 \cdot 2 \equiv 12$， $2^7 \equiv 12 \cdot 2 \equiv 11$， $2^8 \equiv 11 \cdot 2 \equiv 9$，

$2^9 \equiv 9 \cdot 2 \equiv 5$， $2^{10} \equiv 5 \cdot 2 \equiv 10$， $2^{11} \equiv 10 \cdot 2 \equiv 7 \pmod{13}$.

列表为：

2^0	2^1	2^2	2^3	2^4	2^5	2^6	2^7	2^8	2^9	2^{10}	2^{11}
1	2	4	8	3	6	12	11	9	5	10	7

定理 4.1.3 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 $d \equiv k \pmod{ord_m(a)}$.

证 根据定理 1.1.11（欧几里德除法），存在整数 q，r 和 q'，r'使得

$$d = ord_m(a)q + r, 0 \le r < ord_m(a),$$

$$k = ord_m(a)q' + r', 0 \le r' < ord_m(a),$$

又 $a^{ord_m(a)} \equiv 1 \pmod m$，故 $a^d \equiv (a^{ord_m(a)})^q a^r \equiv a^r$， $a^k \equiv a^{r'} \pmod m$.

必要性: 若 $a^d \equiv a^k$，则 $a^r \equiv a^{r'} \pmod m$.

由定理 4.1.2，得到 $r=r'$，故 $d \equiv k \pmod{ord_m(a)}$.

充分性: 若 $d \equiv k \pmod{ord_m(a)}$，则 $r = r'$， $a^d \equiv a^k \pmod m$.

因此，结论成立.

例 4.1.9 $2^{2024} \equiv 2^2 \equiv 4 (mod\, 7)$.

因为整数 2 模 7 的阶为$ord_7(2) = 3$, $2024 \equiv 2 (mod\, 3)$.

定理 4.1.4 设 m>1 是整数，a 是与 m 互素的整数. 设 $d \ge 0$ 为整数，则

$$ord_m(a^d) = \frac{ord_m(a)}{(ord_m(a), d)}.$$

证 因为 $a^{d\ ord_m(a^d)} = (a^d)^{ord_m(a^d)} \equiv 1 \pmod m$，

根据定理 4.1.1，$ord_m(a) | d\ \ ord_m(a^d)$，从而

$$\frac{ord_m(a)}{(ord_m(a),d)} \mid ord_m(a^d) \cdot \frac{d}{(ord_m(a),d)}.$$

因为$\left(\frac{ord_m(a)}{(ord_m(a),d)}, \frac{d}{(ord_m(a),d)}\right) = 1$，所以

$$\frac{ord_m(a)}{(ord_m(a),d)} \mid ord_m(a^d).$$

另一方面，我们有

$$(a^d)^{\frac{ord_m(a)}{(ord_m(a),d)}} = (a^{ord_m(a)})^{\frac{d}{(ord_m(a),d)}} \equiv 1 (\bmod m),$$

根据定理 4.1.1，

$$ord_m(a^d) \mid \frac{ord_m(a)}{(ord_m(a),d)}.$$

因此

$$ord_m(a^d) = \frac{ord_m(a)}{(ord_m(a),d)}.$$

例 4.1.10 整数$2^4 \equiv 3(mod\ 1\,3)$的阶为$ord_{13}(2^4) = \frac{ord_{13}(2)}{(ord_{13}(2),4)} = \frac{12}{(12,\ 4)} = 3.$

推论 4.1.4 设 m>1 是整数，g 是模 m 的原根. 设 $d \geq 0$ 为整数，则 g^d 是模 m 的原根当且仅当$(d, \varphi(m)) = 1$.

证 根据定理 4.1.4，我们有

$$ord_m(g^d) = \frac{ord_m(g)}{(ord_m(g),d)} = \frac{\varphi(m)}{(\varphi(m),d)}.$$

因此，g^d 是模 m 的原根，即$ord_m(g^d) = \varphi(m)$，当且仅当$(d, \varphi(m)) = 1$.

定理 4.1.5 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 4.1.2，$\varphi(m)$ 个数 $g, g^2, \cdots, g^{\varphi(m)}$ 构成模 m 的一个简化剩余系.

又根据推论 4.1.4，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.

推论 4.1.5 设 m>1 是整数，且模 m 存在一个原根，设

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

则整数 $a, (a, m) = 1$ 是模 m 原根的概率是

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

证 根据定理 4.1.5，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，我们有

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

因此，结论成立.

例 4.1.11 求出模 13 的所有原根

解 由例 4.1.6 知道 2 是模 17 的原根.

再根据定理 4.1.5，得到$\varphi(\varphi(13)) = \varphi(12) = 4$个整数.

2, $2^5 \equiv 6$, $2^7 \equiv 11$, $2^{11} \equiv 7$ (mod 13) 是模 13 的全部原根.

定理 4.1.6 设 m>1 是整数，a，b 都是与 m 互素的整数，如果 $(ord_m(a), ord_m(b)) = 1$，则 $ord_m(ab) = ord_m(a)ord_m(b)$. 反之亦然.

证 因为 $(a, m) = 1$, $(b, m) = 1$，所以 $(ab, m) = 1$，且存在 $ord_m(ab)$.

因为

$$\begin{aligned} a^{ord_m(b)ord_m(ab)} &\equiv (a^{ord_m(b)})^{ord_m(ab)}(b^{ord_m(b)})^{ord_m(ab)} \\ &\equiv ((ab)^{ord_m(ab)})^{ord_m(b)} \\ &\equiv 1 (\bmod m) \end{aligned},$$

因此，$ord_m(a) \mid ord_m(b)ord_m(ab)$，但 $(ord_m(a), ord_m(b)) = 1$，

则有 $ord_m(a) \mid ord_m(ab)$.

同理，$ord_m(b) \mid ord_m(ab)$.

再由 $(ord_m(a), ord_m(b)) = 1$ 得到，$ord_m(a)ord_m(a) \mid ord_m(ab)$.

另一方面，我们有

$$(ab)^{ord_m(a)ord_m(b)} = (a^{ord_m(a)})^{ord_m(b)}(a^{ord_m(b)})^{ord_m(a)} \equiv 1 (\bmod m).$$

从而 $ord_m(ab) \mid ord_m(a)ord_m(b)$.

故 $ord_m(ab) = ord_m(a)ord_m(b)$.

反过来，如果 $ord_m(ab) = ord_m(a)ord_m(b)$，那么由

$$(ab)^{[ord_m(a),ord_m(b)]} = a^{[ord_m(a),ord_m(b)]}b^{[ord_m(a),ord_m(b)]} \equiv 1 (\bmod m)$$

推得 $ord_m(ab) \mid [ord_m(a), ord_m(b)]$,

即 $ord_m(a)ord_m(b) \mid [ord_m(a), ord_m(b)]$.

因此 $(ord_m(a), ord_m(b)) = 1$.

结论成立.

注： 对于模 m，不一定有 $ord_m(ab) = [ord_m(a), ord_m(b)]$ 成立. 例如，

$$ord_{14}(3 \cdot 3) = 3 \neq [ord_{14}(3), ord_{14}(3)] = 6.$$

$$ord_{14}(3 \cdot 5) = 1 \neq [ord_{14}(3), ord_{14}(5)] = 6.$$

但有

$$ord_{14}(11 \cdot 13) = ord_{14}(3) = 6 = [ord_{14}(11), ord_{14}(13)] = [3, 2] = 6.$$

例 4.1.12 求模 23 的原根.

解 计算整数 2 模 23 的阶为 $ord_{23}(2) = 11$；

因此，整数-2 为模 23 的原根.

事实上，因为-2 模 23 的阶为 $ord_{23}(-2) = ord_{23}(-1)ord_{23}(2) = 22$.

定理 4.1.7 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 $ord_n(a) \mid ord_m(a)$.

(*ii*) 若 $(m, n) = 1$，则 $ord_{mn}(a) = [ord_m(a), ord_n(a)]$.

证 (*i*) 根据 $ord_m(a)$ 的定义，我们有 $a^{ord_m(a)} \equiv 1 (\bmod m)$.

因此，当 $n \mid m$ 时，可以推出 $a^{ord_m(a)} \equiv 1 (\bmod n)$.

根据定理 4.1.1，我们得到 $ord_n(a) \mid ord_m(a)$.

(*ii*) 由(*i*)我们有 $ord_m(a) \mid ord_{mn}(a), \quad ord_n(a) \mid ord_{mn}(a)$.

从而，$[ord_m(a), ord_n(a)] \mid ord_{mn}(a)$.

又由 $a^{[ord_m(a),ord_n(a)]} \equiv 1 (\bmod m), \quad a^{[ord_m(a),ord_n(a)]} \equiv 1 (\bmod n)$ 及性质 2.1.7 可推出 $a^{[ord_m(a),ord_n(a)]} \equiv 1 (\bmod mn)$.

从而，$ord_{mn}(a)\,|\,[ord_m(a),ord_n(a)]$，故

$$ord_{mn}(a)=[ord_m(a),ord_n(a)].$$

推论 4.1.6　设 p，q 是两个不同的奇素数，a 是与 pq 互素的整数，则

$$ord_{pq}(a)=[ord_p(a),ord_q(a)].$$

推论 4.1.7　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

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

时，我们有 $ord_m(a)=[ord_{2^n}(a),ord_{p_1^{\alpha_1}}(a),\cdots,ord_{p_k^{\alpha_k}}(a)]$.

定理 4.1.8　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 $ord_{mn}(a)=[ord_m(a_1),ord_n(a_2)]$.

证　考虑同余方程组

$$\begin{cases} x\equiv a_1(\bmod m) \\ x\equiv a_2(\bmod n) \end{cases},$$

根据中国剩余定理，这个同余方程组有唯一解 $x\equiv a(\bmod mn)$.

根据推论 4.1.3，我们有 $ord_m(a)=ord_m(a_1),ord_n(a)=ord_n(a_2)$.

从定理 4.1.7，得出 $ord_{mn}(a)=[ord_m(a),ord_n(a)]=[ord_m(a_1),ord_n(a_2)]$.

在定理 4.1.6 的注记中提到，对于模 m，不一定有 $ord_m(ab)=[ord_m(a),ord_m(b)]$ 成立. 但我们有下面的结论成立.

定理 4.1.9　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

$$ord_m(c)=[ord_m(a),ord_m(b)].$$

证　对于整数 $ord_m(a)$ 和 $ord_m(b)$，存在整数 u，v 满足：

$$u\,|\,ord_m(a),v\,|\,ord_m(b),(u,v)=1$$

使得

$$[ord_m(a),ord_m(b)]=uv.$$

现在令

$$s=\frac{ord_m(a)}{u},t=\frac{ord_m(b)}{v}.$$

根据定理 4.1.4，我们有

$$ord_m(a^s)=\frac{ord_m(a)}{(ord_m(a),s)}=u, ord_m(b^t)=v.$$

再根据定理 4.1.6，我们得到

$$ord_m(a^s b^t)=ord_m(a^s)ord_m(b^t)=uv=[ord_m(a),ord_m(b)].$$

因此，取 $c=a^s b^t \pmod m$，即为所求.

例 4.1.13 设整数 m=3631，m 是素数，我们有 $\varphi(3631)=3630=2\cdot 3\cdot 5\cdot 11^2$, 以及

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

根据定理 4.1.9，取整数 a=3，b=5 以及 u=1210，v=3，这是 s=1，t=11^2，

而整数 $c=a^s b^t=3\cdot 5^{121}\equiv 2623 \pmod{3631}$，阶为

$$[ord_{3631}(3),ord_{3631}(5)]=[1210,363]=3630,$$

因此，c=2623 是模 3631 的原根.

4.2 原根

4.2.1 模 p 原根存在性

首先，我们考虑模为奇素数 p 的情形.

定理 4.2.1 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

$$e_r=ord_p(r), 1\le r\le p-1$$
$$e=[e_1,\cdots,e_{p-1}]$$

那么根据定理 4.1.8，存在整数 g 使得 $g^e\equiv 1 \pmod p$.

因此，$e\mid\varphi(p)=p-1$. 又因为 $e_r\mid e,\quad r=1,\cdots,p-1$,

从而推出同余方程 $x^e\equiv 1 \pmod p$ 有 p-1 个解

$$x\equiv 1,\cdots,p-1 \pmod p.$$

根据定理 3.4.4，我们有 p-1$\le e$，故 g 的阶为 p-1，即 g 是模 p 的原根.

此外，根据推论 4.1.4，当有原根时，有$\varphi(p-1)$个原根.

证二（存在性）

设$d\mid p-1$我们用$F(d)$表示模 p 的简化剩余系中阶为 d 的元素个数.

根据推论 4.1.1，模 p 简化剩余系中每个元素的阶是 p-1 的因数，

所以我们有 $\sum_{d\mid p-1} F(d) = p-1$.

因为模 p 阶为 d 的元素满足同余方程 $x^d - 1 \equiv 0 (\bmod p)$，

根据推论 3.4.3，同余方程 $x^d - 1 \equiv 0 (\bmod p)$ 有 d 个模 p 不同的解.

现在，若 a 是模 p 阶为 d 的元素，

则同余方程 $x^d - 1 \equiv 0 (\bmod p)$ 的解可以表示成 $x \equiv a^0, \cdots, a^{d-1}$.

根据定理 4.1.4，这些数中有 $\varphi(d)$ 个阶为 d 的元素，因此 $F(d) = \varphi(d)$.

而若没有模 p 阶为 d 的元素，则 $F(d) = 0$，

总之，我们有 $F(d) \le \varphi(d)$.

但是，我们又有 $\sum_{d\mid p-1} \varphi(d) = p-1$.

这样，由 $\sum_{d\mid p-1} F(d) = p-1$ 与 $\sum_{d\mid p-1} \varphi(d) = p-1$ 推出 $\sum_{d\mid p-1} (\varphi(d) - F(d)) = 0$

因此，对于所有的正整数$d\mid p-1$，我们有 $F(d) = \varphi(d)$.

特别地，我们有 $F(p-1) = \varphi(p-1)$.

这说明存在模 p 阶为 p-1 的元素，即模 p 的原根存在.

推论 4.2.1 设 p 是奇素数，d 是 p-1 的正因数，则模 p 阶为 d 的元素存在.

4.2.2 模 *m* 原根的存在性

其次, 我们考虑一般情形，给出模 m 的原根存在的充要条件.

定理 4.2.2 模 m 的原根存在的充分必要条件是 m=2，4， p^α， $2p^\alpha$，其中 p 是奇素数.

为了证明模 m 原根存在的充要条件（定理 4.2.2），现需要给出如下一些定理.

定理 4.2.3 设 p 是一个奇素数，g 是模 p 的一个原根，则 g 或者 $g+p$ 是模 p^2 的原根.

证 设 g 模 p^2 的阶为 n，则 $g^n \equiv 1 (\bmod p^2)$.

显然，我们有 $g^n \equiv 1 \pmod p$.

因为 g 是模 p 的一个原根，根据定理 4.1.1，我们得到

$$p-1 = ord_p(g) \mid n.$$

又根据推论 4.1.1，我们有

$$n \mid \varphi(p^2) = p(p-1).$$

因此，$n=p-1$，或者 $n=p$（$p-1$）.

如果 $n = p(p-1) = \varphi(p^2)$，则 g 是 p^2 的原根.

如果 $n=p-1$，则 $g^{p-1} \equiv 1 \pmod{p^2}$.

我们要证明 $g+p$ 是模 p^2 的原根，事实上，我们有

$$\begin{aligned}(g+p)^{p-1} &= g^{p-1} + (p-1)g^{p-2}p + \binom{p-1}{2} g^{p-3}p^2 + \cdots + p^{p-1} \\ &\equiv g^{p-1} + (p-1)g^{p-2}p \pmod{p^2}\end{aligned}.$$

我们有 $(g+p)^{p-1} \equiv 1 + (p-1)g^{p-2}p \equiv 1 - g^{p-2}p \pmod{p^2}$,

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

否则，如果 $(g+p)^{p-1} \equiv 1 \pmod{p^2}$，则有 $g^{p-2}p \equiv 0 \pmod{p^2}$，

进而 $g^{p-2} \equiv 0 \pmod p$，这与 g 是 p 的原根矛盾.

因此 $ord_{p^2}(g+p) = p(p-1) = \varphi(p^2)$.

故 $g+p$ 是模 p^2 的原根.

定理 4.2.4 设 p 是一个奇素数，则对于任意正整数 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，则对于任意正整数 α，g 是模 p^α 的原根.

证（i）我们知道，如果模 p 的原根存在，

由定理 4.2.3 及其证明知道模 p^2 的原根 g 也存在，

并且有 $g^{p-1} \not\equiv 1 \pmod{p^2}$.

我们对于 α 做数学归纳法，来证明关系式

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

$\alpha=2$ 时，命题成立.

假设 $\alpha \ge 2$ 时，命题成立，即 $g^{p^{\alpha-2}(p-1)} \not\equiv 1 \pmod{p^\alpha}$.

这个关系可写成

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

两端做 p 次平方，我们有

$$\begin{aligned}
&g^{p^{\alpha-1}(p-1)}=(1+u_{\alpha-2}p^{\alpha-2})^{p}\\
&=1+\binom{p}{1}u_{\alpha-2}p^{\alpha-1}+\binom{p}{2}(u_{\alpha-2}p^{\alpha-1})^{2}+\cdots+(u_{\alpha-2}p^{\alpha-1})^{p}.\\
&\equiv 1+u_{\alpha-2}p^{\alpha}(\bmod p^{\alpha+1})
\end{aligned}$$

因为 $p\nmid u_{\alpha-2}$，所以 $g^{p^{\alpha-1}(p-1)}\not\equiv 1(\bmod p^{\alpha+1})$.

也就是说，对于 $\alpha+1$ 成立，

根据数学归纳法原理，对于所有整数 $\alpha\geq 2$ 成立.

（ii）设 g 是模 p^{α} 的指数为 d，则 $g^{d}\equiv 1(\bmod p^{\alpha})$，从而 $g^{d}\equiv 1(\bmod p^{2})$.

因为 g 是模 p^2 的原根，根据定理 4.1.1，g 模 p^2 的指数 $p(p-1)=\varphi(p^{2})\mid d$，

同时，$d\mid\varphi(p^{\alpha})$，因此，我们可将 d 写成

$$d=p^{r-1}(p-1), 2\leq r\leq\alpha.$$

再将上式代入，得到 $1+u_{r-1}p^{r}=g^{p^{r-1}(p-1)}\equiv 1(\bmod p^{\alpha})$，

或者 $u_{r-1}p^{r}\equiv 0(\bmod p^{\alpha})$.

因为 $p\nmid u_{r-1}$，所以 $r\geq\alpha$. 因此，$r=\alpha$. 就是说，g 是模 p^{α} 的原根.

定理 4.2.5 设 $\alpha\geq 1$，g 是模 p^{α} 的一个原根，则 g 和 $g+p^{\alpha}$ 中的奇数是模 $2p^{\alpha}$ 的一个原根.

证 （i）设奇数 a 满足同余方程 $a^{d}\equiv 1(\bmod p^{\alpha})$.

又显然有 $a^{d}\equiv 1(\bmod 2)$.

根据性质 2.1.7，$a^{d}\equiv 1(\bmod 2p^{\alpha})$.

反之显然.

（ii）若 g 是奇数，令 $d=\varphi(p^{\alpha})$，则 $\varphi(2p^{\alpha})=\varphi(p^{\alpha})=d$.

又当 $g^{d}\equiv 1(\bmod p^{\alpha}), g^{r}\not\equiv 1(\bmod p^{\alpha}), 0<r<d$ 时，有

$$g^{d}\equiv 1(\bmod 2p^{\alpha}), g^{r}\not\equiv 1(\bmod 2p^{\alpha}), 0<r<d.$$

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.

定理 4.2.6 设 a 是一个奇数，则对于任意整数 $\alpha \geq 3$，有

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

证 我们用数学归纳法来证明这个结论，将奇数 a 写成 $a=2b+1$，我们有

$$a^2 = 4b(b+1)+1 \equiv 1(\bmod 2^3).$$

因此，结论对于 $\alpha = 3$ 成立.

假设对于 $\alpha - 1$，结论也成立，即 $a^{2^{(\alpha-1)-2}} \equiv 1(\bmod 2^{\alpha-1})$.

或存在整数 $t_{\alpha-3}$ 使得 $a^{2^{(\alpha-1)-2}} = 1 + t_{\alpha-3} 2^{\alpha-1}$.

两端平方，得到

$$a^{2^{\alpha-2}} = (1+2^{\alpha-1}t_{\alpha-3})^2 = 1+(t_{\alpha-3}+2^{\alpha-2}t^2{}_{\alpha-3})2^{\alpha} \equiv 1(\bmod 2^{\alpha}).$$

这就是说，结论对 α 成立.

根据数学归纳法原理，同余方程对于所有 $\alpha \geq 3$ 成立.

注：定理 4.2.6 说明对于任意整数 $\alpha \geq 3$，模 2^{α} 没有原根.

下面给出定理 4.2.2 的证明.

证 必要性. 设 m 的标准分解式为 $m = 2^{\alpha} p_1^{\alpha_1} \cdots p_k^{\alpha_k}$.

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

根据定理 2.2.13（欧拉定理）及定理 4.2.6，我们有

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

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

令 $h = [\tau, \varphi(p_1^{\alpha_1}), \cdots, \varphi(p_k^{\alpha_k})]$，对所有整数 $a,(a,m)=1$，我们有

$$a^h \equiv 1(\bmod m).$$

因此，若 $h < \varphi(m)$，则模 m 的原根不存在.

现在讨论何时 $h = \varphi(m) = \varphi(2^{\alpha})\varphi(p_1^{\alpha_1}) \cdots \varphi(p_k^{\alpha_k})$.

（a） 当$\alpha \geq 3$时，$\tau = \dfrac{\varphi(2^\alpha)}{2}$，因此$h \leq \dfrac{\varphi(m)}{2} < \varphi(m)$.

（b） 当$k \geq 2$时，$2 | \varphi(p_1^{\alpha_1}), 2 | \varphi(p_2^{\alpha_2})$，进而

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

因此$h < \varphi(m)$.

（c） 当$\alpha = 2, k = 1$时，$\varphi(2^\alpha) = 2, 2 | \varphi(p_1^{\alpha_1})$.

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

故只有在(α, k)是$(1,0),(2,0),(0,1),(1,1)$四种情形之一，

即只有在 m 是$2, 4, p^\alpha, 2p^\alpha$四数之一时，才有可能$h = \varphi(m)$.

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 4.2.4，模 m 原根存在.

当$m = 2p^\alpha$时，根据定理 4.2.5，模 m 的原根存在.

因此，条件的充分性是成立的.

4.2.3 模 *m* 原根的构造

接下来，给出模 m 原根的构造方法.

定理 4.2.7 设 m>1，$\varphi(m)$的所有不同素因数是$q_1, \cdots, q_k$，则 g 是模 m 的一个原根的充分必要条件是

$$g^{\varphi(m)/q_i} \not\equiv 1 \pmod m, i = 1, \cdots, k \cdot$$

证 设 g 是模 m 的一个原根，则 g 对模 m 的阶是$\varphi(m)$，但

$$0 < \varphi(m)/q_i < \varphi(m), i = 1, \cdots, k.$$

根据定理 4.1.2，我们有

$$g^{\varphi(m)/q_i} \not\equiv 1 \pmod m, i = 1, \cdots, k$$

反过来，若 g 对模 m 的阶$e < \varphi(m)$，则根据定理 4.1.1，我们有$e | \varphi(m)$.

因而，存在一个素数 q 使得 $q\,|\,\frac{\varphi(m)}{e}$，即

$$\frac{\varphi(m)}{e}=qu \quad 或 \quad \frac{\varphi(m)}{q}=ue.$$

进而

$$g^{\varphi(m)/q}=(g^{e})^{u}\equiv 1(\bmod m)\cdot$$

与假设矛盾.

例 4.2.1 求模 41 的所有原根.

解 因为 $\varphi(m)=\varphi(41)=40=2^{3}\cdot 5$，所以 $\varphi(m)$ 的素因数为 $q_1=2, q_2=5$，

进而，只需证明：g^{20}, g^{8} 模 m 是否同余于 1，

对于 2, 3……40，等逐个验算：

$$\begin{aligned}&2^{8}\equiv 10, 2^{20}\equiv 1, 3^{8}\equiv 1, 4^{8}\equiv 18, 4^{20}\equiv 1,\\&5^{8}\equiv 18, 5^{20}\equiv 1, 6^{8}\equiv 10, 6^{20}\equiv 40(\bmod 41)\end{aligned}.$$

故 6 是模 41 的原根.

进一步，$(d,\varphi(m))=1$ 时，$ord_m(g^{d})=ord_m(g)$，

因此，当 d 遍历模 $\varphi(m)=40$ 的简化剩余系：

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

共 $\varphi(\varphi(m))=16$ 个数时，6^{d} 遍历模 41 的所有原根：

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

例 4.2.2 求模 43 的原根.

解 设 m=43，则

$$\varphi(m)=\varphi(43)=2\cdot 3\cdot 7, q_1=2, q_2=3, q_3=7.$$

因此，

$$\varphi(m)/q_1=21, \varphi(m)/q_2=14, \varphi(m)/q_3=6.$$

这样，只需证明：g^{21}, g^{14}, g^{6} 模 m 是否同余于 1.

对 2，3，…逐个验算：

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

因此，3 是模 43 的原根.

当 d 遍历模 $\varphi(m)=42$ 的简化剩余系：

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

共 $\varphi(\varphi(43))=12$ 个数时，3^d 遍历模 43 的所有原根：

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

例 4.2.3 设 $m=41^2=1681$，求模 m 的原根.

解 因为已知 6 是模 $p=41$ 的原根，

所以根据定理 4.2.3，可知 6 或者 6+41=47 是模 $41^2=1681$ 的原根.

事实上，我们有

$$6^{40}\equiv 143\equiv 1+41\cdot 3 \pmod{41^2},\quad 47^{40}\equiv 1518\equiv 1+41\cdot 37 \pmod{41^2}.$$

这就是说，

$$6^{40}\not\equiv 1 \pmod{41^2}, 47^{40}\not\equiv 1 \pmod{41^2}.$$

6 和 47 都是模 $m=41^2=1681$ 的原根，它们也是模 41^α 的原根.

由于，$(d,\varphi(m))=1$ 时，$ord_m(g^d)=ord_m(g)$，

因此，当 d 遍历模 $\varphi(41^2)=1640$ 的简化剩余系时，6^d 遍历模 41^2 的所有原根.

例 4.2.4 设 $m=2\cdot 41^2=3362$，求模 m 的原根.

解 这里应用定理 4.2.5 及例 4.2.3，

即可得到 $6+41^2=1687$ 和 47 (是两个奇数)是模 $2\cdot 41^2=3362$ 的原根.

4.2.4 指标与 n 次同余方程

本小节利用原根引入指标的概念，并应用指标的性质研究同余方程 $x^n\equiv a \pmod m$, $(a, m)=1$ 有解的条件及解数.

根据定理 4.1.2 可知, 当 r 遍历模 $\varphi(m)$ 的最小完全剩余系时, 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, $1\le r\le \varphi(\mathrm{m})$, 使得

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

其中 g 是模 m 的一个原根.

定义 4.2.1 设 $m>1$ 是整数，g 是模 m 的一个原根. 设 a 是与 m 互素的整数, 则存在唯一的整数 r 使得

$$g^r\equiv a \pmod m,\ 1\le r\le \varphi(\mathrm{m})$$

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 $r = \mathrm{ind}a$).

注：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 $g^r\equiv a \pmod m$ (**离散对数问题**) 却非常困难.

根据上述定义，我们可以得到如下结论.

定理 4.2.8 设 $m>1$ 是整数, g 是模 m 的一个原根, a 是与 m 互素的整数, 则同余方程 $x^n\equiv a \pmod m$有解的充要条件是

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

且在有解的情况下, 解数为 $(n,\ \varphi(m))$.

证 若同余方程 $x^n\equiv a \pmod m$ 有解 $x\equiv x_0 \pmod m$, 则分别存在非负整数 u, r 使得 $x_0\equiv g^u$, $a\equiv g^r \pmod m$.进而, $g^{un}\equiv g^r \pmod m$, 即有 $un\equiv r \pmod{\varphi(m)}$.

亦即同余方程 $nX\equiv r \pmod{\varphi(m)}$有解 $X\equiv u \pmod{\varphi(m)}$. 因此, $(n,\ \varphi(m)) \mid \mathrm{ind}_g a$ 成立.

反过来, 若 $(n,\ \varphi(m)) \mid \mathrm{ind}_g a$ 成立, 则同余方程 $nX\equiv r \pmod{\varphi(m)}$ 有解 $X\equiv u \pmod{\varphi(m)}$ 且解数为 $(n,\ \varphi(m))$. 因此, 同余方程 $x^n\equiv a \pmod m$有解且解数为$(n,\ \varphi(m))$.

由此，类似于二次剩余，我们可以给出如下定义.

定义 4.2.2 设 $m>1$ 是整数，a 是与 m 互素的整数, 如果 n 次同余方程

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

有解, 则称 a 为模 m 的 ***n* 次剩余**；否则, 称 a 为模 m 的 ***n* 次非剩余**.

进而，我们得到如下推论.

推论 4.2.2　在定理 4.2.8 的假设条件下，a 是模 m 的 n 次剩余的充要条件是

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

证　由定理 4.2.8 的证明知，

同余方程 $x^n\equiv a \pmod{m}$有解的充要条件是同余方程 $nX\equiv r \pmod{\varphi(m)}$ 有解.

而这等价于$(n,\ \varphi(m))\mid \mathrm{ind}_g a$,其中 g 是模 m 的一个原根，也即 $\mathrm{ind}_g a\equiv 0 \pmod{d}$.

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

这等价于 $a^{\frac{\varphi(m)}{d}}\equiv 1 \pmod{m},\ d=(\mathrm{n},\ \varphi(m))$.

结论成立.