第五章 原根与指标
2015年05月12日

信息安全数学基础

陈恭亮　教授 博士生导师

上海交通大学信息安全工程学院

chengl@sjtu.edu.cn

原根与指标 本章要讨论的主要内容:

1. 高次同余式
2. 指数
3. 基本性质(循环群)
4. 原根存在性
5. 原根的构造或生成元的构造
6. 指标
7. n 次剩余
8. 乘法表的构造

序列$s(a)=\{a_k=a^k \mod m \mid k\in\mathbf{N}\}$ 的周期性问题:

一、序列$s(a)$ 是周期序列吗?

二、如何证明序列$s(a)$ 是周期序列?

三、如何找到序列$s(a)$ 的一个周期?

四、如何确定序列$s(a)$ 的最小周期p(a)?

五、如何确定序列两个序列$s(a)$ 和$s(b)$ 的共同的最小周期$p(a,b)$?以及$p(a,b)=[p(a),p(b)]$?

六、是否存在序列$s(c)$ 使得$p(c)=[p(a),p(b)]$?

七、设$a_1,a_2,\cdots,a_t$ 模m 两两不同余, 问是否存在序列$s(c)$ 使得其最小周期$p(c)=[p(a_1),p(a_2),\cdots,p(a_t)]$?

八、可否具体计算出$p(c)=[p(a_1),p(a_2),\cdots,p(a_t)]$?

九、何时模m 原根存在? 即存在g 使得$p(g)=\varphi(m)$?

十、如何求模p 原根g ?

十一、如何求模p^2 原根g ? 如何求模p^α 原根g ?

5.1.1 指数

设$m > 1$ 是整数, a 是正整数. 当$(a, m) = 1$, 根据理2.4.1 (欧拉定理), 有

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

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.

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

$$a^e \equiv 1 \pmod m \qquad (1)$$

成立的最小正整数e 叫做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 叫做模m 的**原根**.

注1 根据定义5.1.1, 我们只能逐个计算

$$a^k \pmod m, \quad k = 1, 2, \ldots, e \qquad (2)$$

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$u = \{u_k = a^k \mod m \mid k \geq 1\}$ 的最小周期$p(u)$.

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

$$\begin{aligned} &1^1 \equiv 1, && 2^3 = 8 \equiv 1, && 3^3 = 27 \equiv -1, \\ &4^3 \equiv (-3)^3 \equiv 1, && 5^3 \equiv (-2)^3 \equiv -1, && 6^2 \equiv (-1)^2 \equiv 1 \pmod 7. \end{aligned}$$

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$\varphi(14) = 6$. 我们有

$$\begin{aligned} &1^1 \equiv 1, && 3^3 = 27 \equiv -1, && 5^3 = 125 \equiv -1, \\ &9^3 \equiv (-5)^3 \equiv 1, && 11^3 \equiv (-3)^3 \equiv 1, && 13^2 \equiv (-1)^2 \equiv 1 \pmod{14}. \end{aligned}$$

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$\varphi(15) = 8$. 我们有

$$\begin{array}{lll} 1^1 \equiv 1, & 2^4 = 16 \equiv 1, & 4^2 = 16 \equiv 1, \\ 7^2 = 49 \equiv 4, & 7^4 \equiv 16 \equiv 1, & 8^4 \equiv (-7)^4 \equiv 1, \\ 11^2 \equiv (-4)^2 \equiv 1, & 13^4 \equiv (-2)^4 \equiv 1, & 14^2 \equiv (-1)^2 \equiv 1 \pmod{15}. \end{array}$$

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$\varphi(9) = 6$. 我们有

$$\begin{aligned} &1^1 \equiv 1, && 2^3 = 8 \equiv -1, && 4^3 = 64 \equiv 1, \\ &5^3 \equiv (-4)^3 \equiv -1, && 7^3 \equiv (-2)^3 \equiv 1, && 8^2 \equiv (-1)^2 \equiv 1 \pmod 9. \end{aligned}$$

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$\varphi(8) = 4$. 我们有

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

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$(5,2)=1$, 所以我们有

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

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$p(u)$, 我们有

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

$$a^d \equiv 1 \pmod{m} \tag{3}$$

的充分必要条件是

$$\mathrm{ord}_m(a) \mid d. \tag{4}$$

证 充分性. 设(4) 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, 我们有

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

必要性. 反证法. 如果(4) 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,

$$a^r \equiv (a^{\mathrm{ord}_m(a)})^q \cdot a^r = a^d \equiv 1 \pmod{m}.$$

这与$\mathrm{ord}_m(a)$ 的最小性矛盾. 故(4) 成立. 证毕

推论1 设$m > 1$ 是整数, a 是与m 互素的整数. 则

$$\mathrm{ord}_m(a) \mid \varphi(m). \tag{5}$$

证 根据欧拉定理(定理2.4.1), 我们有

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

由定理5.1.1, 我们有(5). 证毕

注 根据推论1 (5) , 整数a 模m 的指数$\mathrm{ord}_m(a)$ 是$\varphi(m)$ 的因数, 所以我们可以在$\varphi(m)$ 的因数中求$\mathrm{ord}_m(a)$. 与根据定义5.1.1 求指数$\mathrm{ord}_m(a)$ (2) 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$\varphi(17) = 16$, 所以我们只需对16 的因数$d = 1,\ 2,\ 4,\ 8,\ 16$, 计算$a^d \pmod{m}$. 因为

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

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$\frac{p-1}{2}$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), 我们有

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

根据推论1, 整数a 模p 的指数$\mathrm{ord}_p(a)$ 是$\varphi(p) = p-1 = 2\cdot\frac{p-1}{2}$ 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$b \equiv a \pmod m$, 则$\text{ord}_m(b) = \text{ord}_m(a)$.
(ii) 设a^{-1} 使得$a^{-1} \cdot a \equiv 1 \pmod m$, 则$\text{ord}_m(a^{-1}) = \text{ord}_m(a)$.
证 (i) 若$b \equiv a \pmod m$, 则

$$b^{\text{ord}_m(a)} \equiv a^{\text{ord}_m(a)} \equiv 1 \pmod m,$$

根据定理5.1.1 (4), 我们有$\text{ord}_m(b) \mid \text{ord}_m(a)$.
同样, 我们有$\text{ord}_m(a) \mid \text{ord}_m(b)$. 故$\text{ord}_m(b) = \text{ord}_m(a)$.
(ii)因为

$$(a^{-1})^{\text{ord}_m(a)} \equiv (a^{\text{ord}_m(a)})^{-1} \equiv 1 \pmod m,$$

根据定理5.1.1 (4), 我们有$\text{ord}_m(a^{-1}) \mid \text{ord}_m(a)$.
同样, 我们有$\text{ord}_m(a) \mid \text{ord}_m(a^{-1})$. 故$\text{ord}_m(a^{-1}) = \text{ord}_m(a)$. 证毕
例5.1.8 整数39 模17 的指数为$\text{ord}_{17}(39) = \text{ord}_{17}(5) = 16$. 整数7 模17 的指数为16 . 因为$5^{-1} \equiv 7 \pmod m$.

定理5.1.2 设$m > 1$ 是整数, a 是与m 互素的整数. 则

$$1 = a^0,\ a,\ \ldots,\ a^{\mathrm{ord}_m(a)-1} \tag{6}$$

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

$$1 = a^0,\ a,\ \ldots,\ a^{\varphi(m)-1} \tag{7}$$

组成模m 的简化剩余系.

证 反证法. 如果(6) 中有两个数模m 同余, 则存在整数$0 \le k,\ l < \mathrm{ord}_m(a)$ 使得

$$a^k \equiv a^l \pmod{m}.$$

不妨设$k > l$. 则由$(a, m) = 1$ 和定理2.1.8, 得到

$$a^{k-l} \equiv 1 \pmod{m}.$$

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$\mathrm{ord}_m(a) = \varphi(m)$, 则我们有$\varphi(m)$ 个数(7), 即

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

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$a = g^d$, 我们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$a \leftrightarrow g^d$, 我们也可以空间换时间的方式来提高运算效率, 如计算(参见(**??**))

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

例5.1.9 整数$\{5^k \mid k = 0, \ldots, 15\}$ 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:

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

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, 我们有

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

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

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

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 $2^{1000000} \equiv 2^{10} \equiv 100 \pmod{231}$.

因为整数2 模231 的指数为$\mathrm{ord}_{231}(2) = 30$, $1000000 \equiv 10 \pmod{30}$.

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

$$\mathrm{ord}_m(a^d) = \frac{\mathrm{ord}_m(a)}{(d, \mathrm{ord}_m(a))}. \tag{8}$$

证 因为 $a^{d\,\mathrm{ord}_m(a^d)} = (a^d)^{\mathrm{ord}_m(a^d)} \equiv 1 \pmod m$,
根据定理5.1.1, $\mathrm{ord}_m(a) \mid d\,\mathrm{ord}_m(a^d)$. 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$\left(\frac{\mathrm{ord}_m(a)}{(d, \mathrm{ord}_m(a))}, \frac{d}{(d, \mathrm{ord}_m(a))}\right) = 1$, 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, 我们有 $(a^d)^{\frac{\mathrm{ord}_m(a)}{(d,\mathrm{ord}_m(a))}} = (a^{\mathrm{ord}_m(a)})^{\frac{d}{(d,\mathrm{ord}_m(a))}} \equiv 1 \pmod m$,
根据定理5.1.1, $\mathrm{ord}_m(a^d) \mid \frac{\mathrm{ord}_m(a)}{(d,\mathrm{ord}_m(a))}$.
因此, 我们有(8). 证毕

例5.1.12 整数$5^2 \equiv 8 \pmod{17}$ 模17 的指数为

$$\mathrm{ord}_{17}(5^2) = \frac{\mathrm{ord}_{17}(5)}{(2, \mathrm{ord}_{17}(5))} = 8.$$

推论1 设$m > 1$ 是整数, g 是模m 的原根. 设$d \geq 0$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 (8), 我们有

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

因此, g^d 是模的原根, 即$\mathrm{ord}_m(g^d) = \varphi(m)$ 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

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

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

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

因此, $\dfrac{\mathrm{ord}_m(a)}{k} \mid d$. 再令 $\quad d=q\cdot\frac{\mathrm{ord}_m(a)}{k}, \quad 1\le q\le k$.

由

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

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 (7), $\varphi(m)$ 个整数

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

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

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

则整数a, $(a, m) = 1$ 是模m 原根的概率是

$$\frac{\varphi(\varphi(m))}{\varphi(m)} = \prod_{i=1}^{s}(1 - \frac{1}{p_i}). \tag{9}$$

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, 我们有

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

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 知道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的构造.

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

$$\mathrm{ord}_m(a \cdot b) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b). \tag{10}$$

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

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

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

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

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

$$\mathrm{ord}_{mn}(a) = [\mathrm{ord}_m(a), \mathrm{ord}_n(a)]. \tag{11}$$

证 (i) 根据$\mathrm{ord}_m(a)$ 的定义, 我们有 $a^{\mathrm{ord}_m(a)} \equiv 1 \pmod m$.
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, 我们得到 $\mathrm{ord}_n(a) \mid \mathrm{ord}_m(a)$.
(ii) 由(i) 我们有 $\mathrm{ord}_m(a) \mid \mathrm{ord}_{mn}(a)$, $\mathrm{ord}_n(a) \mid \mathrm{ord}_{mn}(a)$,
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(11) 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

$$\mathrm{ord}_{p \cdot q}(a) = [\mathrm{ord}_p(a), \mathrm{ord}_q(a)] \mid [p-1, q-1]. \tag{12}$$

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

$$\mathrm{ord}_{p \cdot q}(a) = [\mathrm{ord}_p(a), \mathrm{ord}_q(a)] \mid q-1. \tag{13}$$

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

$$1 < e < \varphi(n),\ (e, \varphi(n)) = 1, \tag{14}$$

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

$$e \cdot d \equiv 1 \pmod{\mathrm{ord}_{pq}(a)}. \tag{15}$$

而且, 对于整数

$$a^e \equiv c \pmod{n}, \quad 1 \le c < n, \tag{16}$$

有

$$c^d \equiv a \pmod{n}. \tag{17}$$

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$d = d_a$, $1 \le d < \mathrm{ord}_{pq}(a)$, 使得(15) 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

$$a^{\mathrm{ord}_p(a)} \equiv 1 \pmod{p}. \tag{18}$$

根据定理5.1.6之推论1, $\dfrac{\mathrm{ord}_{pq}(a)}{\mathrm{ord}_p(a)}$ 为整数. 在(18) 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(17) 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, 我们有

$$\mathrm{ord}_m(a) = [\mathrm{ord}_{2^n}(a), \mathrm{ord}_{p_1^{\alpha_1}}(a), \ldots, \mathrm{ord}_{p_k^{\alpha_k}}(a)]. \tag{19}$$

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

$$\operatorname{ord}_{mn}(a)=[\operatorname{ord}_m(a_1),\operatorname{ord}_n(a_2)]. \tag{20}$$

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), 这个同余式组有惟一解

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

根据性质5.1.1 (i), 我们有

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

因此, 从定理5.1.7 得到,

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

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

$$\mathrm{ord}_m(c) = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)]. \tag{21}$$

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, 我们有

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

再根据定理5.1.6, 我们得到

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

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. 我们有$\varphi(3631) = 3630 = 2\cdot 3\cdot 5\cdot 11^2$, 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$s = 1$, $t = 11^2$, 我们有整数$c = a^s\cdot b^t = 3^1\cdot 5^{121} \equiv 2623 \pmod{3631}$的指数为

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

因此, $c = 2623$ 是模3631 的原根.

访问主页

标题页

目录页

返回

全屏显示

关闭

退出

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

$$a_k^e \equiv 1 \pmod{m}, \quad 1 \le k \le \varphi(m) \tag{22}$$

成立的最小正整数. 则存在整数a 使得

$$e = \mathrm{ord}_m(a) = [\mathrm{ord}_m(a_1), \mathrm{ord}_m(a_2), \ldots, \mathrm{ord}_m(a_{\varphi(m)})] \tag{23}$$

证 应用定理5.1.9, 可归纳得到: 存在整数a 使得

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

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$\mathrm{ord}_m(a_k) \mid e$, $1 \le k \le \varphi(m)$. 所以

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

另一方面, 对每个a_k, 有 $a_k^{[\mathrm{ord}_m(a_1),\ldots,\mathrm{ord}_m(a_{\varphi(m)})]} = \left((a_k)^{\mathrm{ord}_m(a_k)}\right)^{[\mathrm{ord}_m(a_1),\ldots,\mathrm{ord}_m(a_{\varphi(m)})]/\mathrm{ord}_m(a_k)} \equiv 1 \pmod{m}$
根据e 的最小性, 有$e \le [\mathrm{ord}_m(a_1), \ldots, \mathrm{ord}_m(a_{\varphi(m)})]$. 因此(23) 成立. 证毕

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

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

当$m = p$ 是素数时, 我们有

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