

初等数论

第五章 原根与指标

中山大学 数据科学与计算机学院

1. 指数

根据欧拉定理, 当 a 与 m ($m > 1$)互素时, 有 $a^{\varphi(m)} \equiv 1 \pmod{m}$ 成立,

1.1. 指数

设 $m > 1$ 是整数, a 是与 m 互素的正整数(即 a 处于模 m 的一个简化剩余系中), 称使得

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

的最小正整数 e 为 a 对模 m 的指数(或阶), 记作 $\text{ord}_m(a)$

如果 a 对模 m 的指数是 $\varphi(m)$, 这时称 a 为模 m 的原根.

示例: $m = 7, \varphi(m) = 6$,

对 $a = 1$ 来说, $1^1 = 1$, 所以 a 的指数为1

对 $a = 2$ 来说, $2^1 = 2, 2^2 = 4, 2^3 \equiv 1 \pmod{7}$, 所以2的指数为3

对 $a = 3$ 来说, $3^1 = 3, 3^2 \equiv 2, \dots, 3^6 \equiv 1 \pmod{7}$, 所以3的指数为6

类似计算, 4的指数为3, 5的指数为6, 6的指数为2.

可见上述只有3,5是模7的原根

示例: $m = 15, \varphi(m) = 8$

1 ~ 5的数中与15互素的数有1,2,4,7,8,11,13,14

类似上述计算可以看出它们的指数分别为:

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

可见没有模15的原根. 或者说"并不是对于任意大于1的整数 m 都有模 m 的原根".

1.2. 指数的性质

定理

设 m 是大于1的整数, a 与 m 互素. 整数 d 使得 $a^d \equiv 1 \pmod m$ 当且仅当 $\text{ord}_m(a) \mid d$.

"必要性:"

$$\text{ord}_m(a) \mid d \implies d = k \cdot \text{ord}_m(a) \implies a^d = (a^{\text{ord}_m(a)})^k \implies a^d \equiv 1 \pmod m$$

"充分性:" 假设 d 使得 $a^d \equiv 1 \pmod m$,

如果 $\text{ord}_m(a) \nmid d$, 则由欧几里德除法知, 存在整数 q, r 使得

$$d = q \cdot \text{ord}_m(a) + r, \quad 0 < r < \text{ord}_m(a)$$

从而

$$a^d \equiv a^r \cdot (a^{\text{ord}_m(a)})^q \pmod m$$

而

$$a^d \equiv 1 \pmod m$$

从而 $a^r \equiv 1 \pmod m$, 但这就与指数的定义矛盾.

根据欧拉定理, 如果 a 与 m 互素, $\varphi(m)$ 使得 $a^{\varphi(m)} \equiv 1 \pmod{m}$, 因此有 $\text{ord}_m(a) \mid \varphi(m)$.
 a 对模 m 的指数必定是 $\varphi(m)$ 的因子, 所以为了求 a 的指数, 只需要在 $\varphi(m)$ 的因子中找.

示例: 求 $\text{ord}_{17}(5)$

因为 $\varphi(17) = 16$ 的因子是1,2,4,8,16,

检查 $5^1, 5^2, 5^4, 5^8, 5^{16}$,

可以发现只有 $5^{16} \equiv 1 \pmod{17}$

所以 $\text{ord}_{17}(5) = 16$, 从而5是模17的原根.

定理

设 m 是大于1的整数, a 与 m 互素. 如果 $n \mid m$, 则 $\text{ord}_n(a) \mid \text{ord}_m(a)$.

$$\left. \begin{array}{l} a^{\text{ord}_m(a)} \equiv 1 \pmod{m} \\ n \mid m \end{array} \right\} \implies a^{\text{ord}_m(a)} \equiv 1 \pmod{n} \implies \text{ord}_n(a) \mid \text{ord}_m(a)$$

定理

设 m 是大于1的整数, a 与 m 互素. 如果 $b \equiv a \pmod{m}$, 则 $\text{ord}_m(a) = \text{ord}_m(b)$.

事实上, $b \equiv a \pmod{m} \implies a^{\text{ord}_m(b)} \equiv b^{\text{ord}_m(b)} \equiv 1 \pmod{m} \implies \text{ord}_m(a) \mid \text{ord}_m(b)$.
类似地, $b \equiv a \pmod{m} \implies b^{\text{ord}_m(a)} \equiv a^{\text{ord}_m(a)} \equiv 1 \pmod{m} \implies \text{ord}_m(b) \mid \text{ord}_m(a)$.
所以有, $\text{ord}_m(a) = \text{ord}_m(b)$.

例如,

$$39 \equiv 5 \pmod{17} \implies \text{ord}_{17}(39) = \text{ord}_{17}(5) = 16.$$

定理

设 m 是大于1的整数, a 与 m 互素. 如果 $ab \equiv 1 \pmod{m}$, 则 $\text{ord}_m(a) = \text{ord}_m(b)$.

事实上

$$\begin{aligned}(ab)^{\text{ord}_m(a)} &\equiv 1 \pmod{m} \implies a^{\text{ord}_m(a)} \cdot b^{\text{ord}_m(a)} \equiv 1 \pmod{m} \\ &\implies b^{\text{ord}_m(a)} \equiv 1 \pmod{m} \implies \text{ord}_m(b) \mid \text{ord}_m(a).\end{aligned}$$

类似地

$$\begin{aligned}(ab)^{\text{ord}_m(b)} &\equiv 1 \pmod{m} \implies a^{\text{ord}_m(b)} \cdot b^{\text{ord}_m(b)} \equiv 1 \pmod{m} \\ &\implies a^{\text{ord}_m(b)} \equiv 1 \pmod{m} \implies \text{ord}_m(a) \mid \text{ord}_m(b).\end{aligned}$$

所以有, $\text{ord}_m(a) = \text{ord}_m(b)$.

例如,

$$5 \cdot 7 \equiv 1 \pmod{17} \implies \text{ord}_{17}(7) = \text{ord}_{17}(5) = 16$$

定理

设 m 是大于1的整数, a 与 m 互素.

$$a^0 (= 1), a^1, a^2, \dots, a^{\text{ord}_m(a)-1}$$

模 m 两两不同余.

如果存在 $0 \leq l < k \leq \text{ord}_m(a) - 1$ 使得 $a^k \equiv a^l \pmod{m}$. 又因为 a 与 m 互素, 所以有 $a^{k-l} \equiv 1 \pmod{m}$ 成立, 且 $k-l < \text{ord}_m(a) - 1$. 这就与指数的定义矛盾. \diamond

根据这个结论, 当 $\text{ord}_m(a) = \varphi(m)$ 时, 即 a 是模 m 的原根时,

$$\{a^0, a^1, a^2, \dots, a^{\varphi(m)-1}\}$$

这些数正好构成了模 m 的一个简化剩余系.

例如, $\{5^0, 5^1, \dots, a^{\varphi(m)-1}\}$ 正好是模17的一个简化剩余系, 因为5是模17的一个原根.

定理

设 m 是大于1的整数, a 与 m 互素. $a^k \equiv a^l \pmod{m}$ 当且仅当 $k \equiv l \pmod{\text{ord}_m(a)}$.

根据欧几里德除法, 存在整数 q, r 和 q', r' 使得

$$k = q \cdot \text{ord}_m(a) + r, \quad 0 \leq r < \text{ord}_m(a)$$

和

$$l = q' \cdot \text{ord}_m(a) + r', \quad 0 \leq r' < \text{ord}_m(a)$$

成立, 从而有

$$a^k = a^{\text{ord}_m(a)q+r} \equiv a^r \pmod{m},$$

以及

$$a^l = a^{\text{ord}_m(a)q'+r'} \equiv a^{r'} \pmod{m}$$

成立.

"必要性:" $a^k \equiv a^l \pmod{m} \implies a^r \equiv a^{r'} \pmod{m}$, 于是 $r = r'$, 所以 $k \equiv l \pmod{\text{ord}_m(a)}$

"充分性:" $k \equiv l \pmod{\text{ord}_m(a)} \implies r = r' \implies a^k \equiv a^l \pmod{m} \quad \diamond$

定理

设 m 是大于1的整数, a 与 m 互素, k 是非负整数. $\text{ord}_m(a^k) = \frac{\text{ord}_m(a)}{(\text{ord}_m(a), k)}$.

证明: 设 $d = (\text{ord}_m(a), k)$. 先证明 $\frac{\text{ord}_m(a)}{d} \mid \text{ord}_m(a^k)$.

$$\because a^{k \cdot \text{ord}_m(a^k)} = (a^k)^{\text{ord}_m(a^k)} \equiv 1 \pmod{m}$$

$$\therefore \text{ord}_m(a) \mid (k \cdot \text{ord}_m(a^k)) \quad \therefore \frac{\text{ord}_m(a)}{d} \mid (\text{ord}_m(a^k) \cdot \frac{k}{d}).$$

又因为 $(\frac{\text{ord}_m(a)}{d}, \frac{k}{d}) = 1$, 所以 $\frac{\text{ord}_m(a)}{d} \mid \text{ord}_m(a^k)$.

另一方面,

$$\because (a^k)^{\frac{\text{ord}_m(a)}{d}} = (a^{\text{ord}_m(a)})^{\frac{k}{d}} \equiv 1 \pmod{m} \quad \therefore \text{ord}_m(a^k) \mid \frac{\text{ord}_m(a)}{d} \quad \diamond$$

例如, 5模17的指数是16, 则 5^2 (即8)模17的指数是 $\frac{16}{(16, 2)} = 8$.

推论

设 m 是大于1的整数, k 是非负整数. 如果 a 是模 m 的原根, 则 $a^k (k > 0)$ 也是模 m 的原根当且仅当 $(k, \varphi(m)) = 1$.

推论

设 m 是大于1的整数. 如果模 m 有原根, 则模 m 的原根的个数为 $\varphi(\varphi(m))$, 且从模 m 的简化剩余中均匀随机选取一个元素是模 m 原根的概率是

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

定理

设 m 是大于1的整数, a, b 都是与 m 互素的整数, r 是 a 的模 m 的指数, s 是 b 的模 m 的指数, t 是 ab 的模 m 的指数, 则 $t = rs$ 当且仅当 r 与 s 互素, 即

$$\text{ord}_m(ab) = \text{ord}_m(a) \cdot \text{ord}_m(b) \iff (\text{ord}_m(a), \text{ord}_m(b)) = 1.$$

证明: "充分性:" 需要说明 t 与 rs 相互整除.

先说明 $t \mid (rs)$: $(ab)^{rs} = a^{rs}b^{rs} = (a^r)^s(b^s)^r \equiv 1 \pmod{m} \implies t \mid (rs)$

再说明 $(rs) \mid t$: 只需要说明 $r \mid t, s \mid t$, 而 r 与 s 互素, 所以 $rs \mid t$. 为此,

$$a^{st} \equiv a^{st}(b^s)^t = (ab)^{st} = [(ab)^t]^s \equiv 1 \pmod{m}$$

$$\therefore r \mid (st)$$

又因为 r 与 s 互素, 所以有 $r \mid t$;

$$b^{rt} \equiv b^{rt}(a^r)^t = (ab)^{rt} = [(ab)^t]^r \equiv 1 \pmod{m}$$

$$\therefore s \mid (rt)$$

又因为 r 与 s 互素, 所以有 $s \mid t$.

下面证明"必要性:"

如果 $t = rs$, 那么

$$\therefore (ab)^{[r,s]} = a^{[r,s]}b^{[r,s]} \equiv 1 \pmod{m}$$

$$\therefore t|[r,s] \quad \therefore (rs)|[r,s] \quad \therefore [r,s] = rs, \quad \therefore (r,s) = 1 \quad \diamond$$

这个结论还说明,

不一定有

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

不一定有

$$\text{ord}_m(ab) = [\text{ord}_m(a), \text{ord}_m(b)]$$

例如, $m = 10, a = b = 3$, 则 $\text{ord}_m(ab) = 2$, 而 $\text{ord}_m(a) = \text{ord}_m(b) = 4$.

定理

设 m 是大于1的整数, a, b 均与 m 互素. 存在 c 使得 $\text{ord}_m(c) = [\text{ord}_m(a), \text{ord}_m(b)]$.

回忆最小公倍数的性质, 存在 u, v 使得

$$u \mid \text{ord}_m(a), v \mid \text{ord}_m(b), uv = [\text{ord}_m(a), \text{ord}_m(b)], (u, v) = 1.$$

令

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

从而

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

这样 a^s 模 m 的指数与 b^t 模 m 的指数互素. 再令 $c = a^s b^t$, 从而有

$$\text{ord}_m(c) = \text{ord}_m(a^s b^t) = \text{ord}_m(a^s) \cdot \text{ord}_m(b^t) = uv = [\text{ord}_m(a), \text{ord}_m(b)]. \quad \diamond$$

一般地, 存在 g 使得 $\text{ord}_m(g) = [\text{ord}_m(a_1), \text{ord}_m(a_2), \dots, \text{ord}_m(a_k)], 2 \leq k \leq \varphi(m)$.

还可以看到, 如果 $(\text{ord}_m(a), \text{ord}_m(b)) = 1$, 则有 $\text{ord}_m(ab) = [\text{ord}_m(a), \text{ord}_m(b)]$. 如果没有该条件, 则存在 c 使得 $\text{ord}_m(c) = [\text{ord}_m(a), \text{ord}_m(b)]$.

定理

设 a, m, n 两两互素, r 是 a 模 m 的指数, s 是 a 模 n 的指数, t 是 a 模 mn 的指数. $t = [r, s]$, 即 $\text{ord}_{mn}(a) = [\text{ord}_m(a), \text{ord}_n(a)]$.

首先, 由于 $m \mid mn, n \mid mn$, 所以有 $r \mid t, s \mid t \implies [r, s] \mid t$. 另一方面,

$$a^r \equiv 1 \pmod{m} \implies a^{[r,s]} \equiv 1 \pmod{m}$$

$$a^s \equiv 1 \pmod{n} \implies a^{[r,s]} \equiv 1 \pmod{n}$$

所以 $a^{[r,s]} \equiv 1 \pmod{mn}$, 从而有 $t \mid [r, s]$. \diamond

(要注意与“ $\text{ord}_m(ab) = [\text{ord}_m(a), \text{ord}_m(b)]$ 未必成立”的区别.)

推论

设 p, q 是两个不同的素数. 如果 a 与 pq 互素, 则 $\text{ord}_{pq}(a) = [\text{ord}_p(a), \text{ord}_q(a)]$. 一般地, 如果 m 的标准分解式为 $m = 2^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s}$, $(a, m) = 1$, 则有

$$\text{ord}_m(a) = [\text{ord}_{2^{\alpha_1}}(a), \text{ord}_{p_2^{\alpha_2}}(a), \dots, \text{ord}_{p_s^{\alpha_s}}(a)].$$

定理

设 m, n 互素, a_1, a_2 均与 mn 互素. 存在 a 使得 $\text{ord}_{mn}(a) = [\text{ord}_m(a_1), \text{ord}_n(a_2)]$.

根据中国剩余定理, 同余式组
$$\begin{cases} x \equiv a_1 \pmod{m} \\ x \equiv a_2 \pmod{n} \end{cases}$$
有唯一解

$$x \equiv (x^{-1} \pmod{m}) \cdot n \cdot a_1 + (m^{-1} \pmod{n}) \cdot m \cdot a_2 \pmod{M}.$$

令 $a = [x^{-1} \pmod{m}] \cdot n \cdot a_1 + [m^{-1} \pmod{n}] \cdot m \cdot a_2$, 显然 $a \equiv a_1 \pmod{m}, a \equiv a_2 \pmod{n}$, 因此,

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

从而

$$\text{ord}_{mn}(a) = [\text{ord}_m(a), \text{ord}_n(a)] = [\text{ord}_m(a_1), \text{ord}_n(a_2)] \quad \diamond$$

可以看出, 如果 $a_1 = a_2$, 则 $\text{ord}_{mn}(a_1) = [\text{ord}_m(a_1), \text{ord}_n(a_1)]$. 如果没有条件 $a_1 = a_2$, 则存在 a 使得 $\text{ord}_{mn}(a) = [\text{ord}_m(a_1), \text{ord}_n(a_2)]$.

与此对比, 如果 $(\text{ord}_m(a), \text{ord}_m(b)) = 1$, 则有 $\text{ord}_m(ab) = [\text{ord}_m(a), \text{ord}_m(b)]$. 如果没有该条件, 则存在 c 使得 $\text{ord}_m(c) = [\text{ord}_m(a), \text{ord}_m(b)]$.

2. 模素数 p 的原根

定理

设 p 是素数, 则模 p 有原根.

证明: 在模 p 的简化剩余系中, 存在 g 使得

$$\text{ord}_p(g) = [\text{ord}_p(1), \text{ord}_p(2), \dots, \text{ord}_p(p-1)].$$

记这个最小公倍数为 δ , 即这个 g 的指数为 δ , 下面证明 $\delta = p-1$, 即 g 是模 p 的原根. 一方面, 对这个 g , 一定有 $g^{p-1} \equiv 1 \pmod{p}$, 从而有 $\delta \leq p-1$.

另一方面, 由于 δ 是 $\text{ord}_p(1), \text{ord}_p(2), \dots, \text{ord}_p(p-1)$ 的公倍数, 所以

$$\text{ord}_p(1) \mid \delta, \text{ord}_p(2) \mid \delta, \dots, \text{ord}_p(p-1) \mid \delta.$$

这表明

$$1^\delta \equiv 1 \pmod{p}, 2^\delta \equiv 1 \pmod{p}, \dots, (p-1)^\delta \equiv 1 \pmod{p}.$$

也就是说, 同余方程

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

至少有 $p-1$ 个解, 从而知道 $\delta \geq p-1$. 所以, $\delta = p-1$.

定理

设 p 是奇素数, q_1, q_2, \dots, q_s 是 $p-1$ 的所有素因数. g 是模 p 原根当且仅当

$$g^{\frac{p-1}{q_i}} \not\equiv 1 \pmod{p}, \quad i = 1, 2, \dots, s.$$

示例: 求模 $p = 23$ 的原根.

这里 $p-1 = 22 = 2 \cdot 11$, $p-1$ 的因子有1, 2, 11, 22.

先求 $a = 2$ 对模23的指数:

$$2^2 \equiv 4 \pmod{23}$$

$$2^{11} = (2^4)^2 \cdot 2^3 \equiv (-7)^2 \cdot 8 \equiv 3 \cdot 8 \equiv 1 \pmod{23}$$

所以 $\text{ord}_{23}(2) = 11$, 2不是模23的原根;

再求 $a = 3$ 对模23的指数:

$$3^2 \equiv 9 \pmod{23}$$

$$3^3 \equiv 4 \pmod{23}$$

$$3^{11} = (3^3)^3 \cdot 3^2 \equiv 4^3 \cdot 9 \equiv (-5) \cdot 9 \equiv 1 \pmod{23}$$

所以 $\text{ord}_{23}(3) = 11$, 3不是模23的原根;

再求 $a = 4$ 对模23的指数:

$$4^2 \equiv -7 \pmod{23}$$

$$4^{11} = (4^4)^2 \cdot 4^3 \equiv 3^2 \cdot (-5) \equiv 1 \pmod{23}$$

所以 $\text{ord}_{23}(4) = 11$, 4不是模23的原根;

再求 $a = 5$ 对模23的指数:

$$5^2 \equiv 9 \pmod{23}$$

$$5^{11} = (5^4)^2 \cdot 5^3 \equiv 4^2 \cdot 10 \equiv 4 \cdot (-6) \equiv -1 \pmod{23}$$

$$5^{22} \equiv 1 \pmod{23}$$

所以 $\text{ord}_{23}(5) = 22$, 5是模23的原根.