

初等数论

第五章 指数 原根 指标

卢伟

Email: luwei3@mail.sysu.edu.cn

中山大学 数据科学与计算机学院

1. 指数

根据欧拉定理我们知道, 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.

1.2. 指数的性质

1. a 与 m 互素, 则整数 d 使得 $a^d \equiv 1 \pmod{m} \iff \text{ord}_m(a) | d$

事实上

" \Leftarrow :"

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

" \implies :" 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.

1-1 由此, 如果 a 与 m 互素, 自然有 $\text{ord}_m(a) | \varphi(m)$.

也就是说, 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.

1-2 设 a 与 m 互素, $n|m \implies \text{ord}_n(a) | \text{ord}_m(a)$

事实上,

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

◇

1-3 $m > 1, (a, m) = 1$, 则 $b \equiv a \pmod{m} \implies \text{ord}_m(a) = \text{ord}_m(b)$; (即 a 所在的简化剩余类中的元素都同阶)

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

类似, 有 $\text{ord}_m(a) | \text{ord}_m(b)$

比如,

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

1-4 $ab \equiv 1 \pmod{m} \implies \text{ord}_m(a) = \text{ord}_m(b)$ (即 a 与它的逆元同阶)

事实上

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

类似可以说明

$$\text{ord}_m(a) \mid \text{ord}_m(b) \quad \diamond$$

比如

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

2, 设 $m > 1, (a, m) = 1$, 则

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

模 m 两两不同余.

事实上, 如果存在 $0 \leq l < k \leq \text{ord}_m(a) - 1$ 使得 $a^k \equiv a^l \pmod{m}$,

因为 a 与 m 互素, 所以有 $a^{k-l} \equiv 1 \pmod{m}$ 成立

这就与指数的定义矛盾. \diamond

2-1 根据这个结论, 当 $\text{ord}_m(a) = \varphi(m)$ 时(即 a 是模 m 的原根),
 $\{a^0 (= 1), a^1, a^2, \dots, a^{\varphi(m)-1}\}$ 这些数正好构成了模 m 的一个简化剩余系.

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

2-2 设 $m > 1, (a, m) = 1$, 则 $a^k \equiv a^l \pmod m \iff k \equiv l \pmod{\text{ord}_m(a)}$

事实上, 根据欧几里德除法, 我们知道, 存在 q, r 和 q', r' 使得

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

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

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

" \implies :" $a^k \equiv a^l \pmod m \implies a^r \equiv a^{r'} \pmod m,$

所以 $r = r'$, 所以 $k \equiv l \pmod{\text{ord}_m(a)}$

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

3, 设 $\text{ord}_m(a) = r, \text{ord}_m(a^k) = r', d = (r, k)$, 则 $r' = \frac{r}{d}$ (即 $\text{ord}_m(a^k) = \frac{\text{ord}_m(a)}{(\text{ord}_m(a), k)}$)

证明: 需要说明左右两边互相整除, 先说明 $\frac{r}{d} | r'$

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

$$\therefore r | (k, r') \quad \therefore \frac{r}{d} | (r' \cdot \frac{k}{d})$$

又因为 $(\frac{r}{d}, \frac{k}{d}) = 1$, 所以 $\frac{r}{d} | r'$. 另一方面,

$$\because (a^k)^{\frac{r}{d}} = (a^r)^{\frac{k}{d}} \equiv 1 \pmod{m} \quad \therefore r' | \frac{r}{d} \quad \diamond$$

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

3-1 根据这个结论, 如果 a 是模 m 的原根(即 a 的指数是 $\varphi(m)$), 则 $a^k (k > 0)$ 也是模 m 的原根 $\iff (k, \varphi(m)) = 1$

3-2 我们知道 a 是模 m 的原根的话, 则 $\{a^0, a^1, a^2, \dots, a^{\varphi(m)-1}\}$ 构成模 m 的一个简化剩余系, 这个简化剩余系中, 模 m 的原根(如果有的话)个数也就是这样的 k 的个数, 而 $0 \sim \varphi(m)$ 之间与 $\varphi(m)$ 互素的数的个数也就是 $\varphi(\varphi(m))$, 所以, 模 m 有 $\varphi(\varphi(m))$ 个原根.

3-3 这样, 从这个简化剩余中任取一个元素是模 m 原根的概率就是

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

4, 设 a, b 都与 m 互素(所以 ab 与 m 互素), 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 $t = rs \iff r$ 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: " \Leftarrow :" 需要说明 t 与 rs 相互整除.

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

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

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

$$\therefore r|(st)$$

又因为 r 与 s 互素, 所以有 $r|t$;

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

$$\therefore s|(rt)$$

又因为 r 与 s 互素, 所以有 $s|t$;

又因为 r 与 s 互素, 所以有 $(rs)|t$.

4, 设 a, b 都与 m 互素(所以 ab 与 m 互素), 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 $t = rs \iff r$ 与 s 互素.

下面说明" \implies :"

假设 $t = rs$,

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

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

4-1 这个结论说明, 一般地, 未必有

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

4-2 事实上, 连下面的式子也未必有

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

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

4-3 已知 a, b 均与 m 互素, 则存在 c 使得 $\text{ord}_m(c) = [\text{ord}_m(a), \text{ord}_m(b)]$.

我们知道结论: 对于正整数 a, b , 存在整数 $a' | a, b' | b$ 使得 $a' \cdot b' = [a, b], (a', b') = 1$, 对 $\text{ord}_m(a), \text{ord}_m(b)$ 使用这个结论: 存在 u, v 使得

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

置

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

从而

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

这样 a^s 模 m 的指数与 b^t 模 m 的指数互素, 置 $c = a^s b^t$, 所以有

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

即: $(\text{ord}_m(a), \text{ord}_m(b)) = 1 \implies \text{ord}_m(ab) = [\text{ord}_m(a), \text{ord}_m(b)]$

如果没有条件 $(\text{ord}_m(a), \text{ord}_m(b)) = 1$, 则存在 c , 使得: $\text{ord}_m(c) = [\text{ord}_m(a), \text{ord}_m(b)]$

注: 这个结论的一般情况是存在 g , 使得:

$$\text{ord}_m(g) = [\text{ord}_m(a_1), \text{ord}_m(a_2), \text{ord}_m(a_3), \dots, \text{ord}_m(a_k)]$$

5, 设 a, m, n 两两互素, 设 r 是 a 模 m 的指数, s 是 a 模 n 的指数, t 是 a 模 mn 的指数, 则 $t = [r, s]$ (即 $(a, m) = (a, n) = (m, n) = 1 \implies \text{ord}_{mn}(a) = [\text{ord}_m(a), \text{ord}_n(a)]$) 事实上, 由性质1-2我们知道

$$r|t, s|t \implies [r, s]|t$$

另一方面,

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

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

$$\therefore a^{[r, s]} \equiv 1 \pmod{mn} \quad (\because a \equiv b \pmod{M}, a \equiv b \pmod{N} \implies a \equiv b \pmod{[M, N]})$$

$$\therefore t|[r, s] \quad \diamond$$

(注意与"式子 $\text{ord}_m(ab) = [\text{ord}_m(a), \text{ord}_m(b)]$ 未必成立"的区别)

5-1 从而, 如果 a 与 pq ($p \neq q$)互素, 显然有

$$\text{ord}_{pq}(a) = [\text{ord}_p(a), \text{ord}_q(a)]$$

5-2 更一般的, 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

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

令

$$\beta \triangleq [\varphi(2^{\alpha_1}), \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})]$$

即 β 是 $\varphi(2^{\alpha_1}), \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})$ 的最小公倍数,

由于 $\text{ord}_{p^\alpha}(a) | \varphi(p^\alpha)$, 从而 β 是 $\text{ord}_{2^{\alpha_1}}(a), \text{ord}_{p_2^{\alpha_2}}(a), \dots, \text{ord}_{p_s^{\alpha_s}}(a)$ 的公倍数, 所以

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

即

$$\text{ord}_m(\alpha) | \beta$$

$$\text{而 } \varphi(2^{\alpha_1}) = \begin{cases} 1 & \alpha_1 = 0 \\ 1 & \alpha_1 = 1 \\ 2 & \alpha_1 = 2 \\ 2^{\alpha_1} - 2^{\alpha_1-1} = 2^{\alpha_1-1} & \alpha_1 \geq 3 \end{cases}$$

所以

$$\beta = \begin{cases} [1, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})] & \alpha_1 = 0 \\ [1, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})] & \alpha_1 = 1 \\ [2, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})] & \alpha_1 = 2 \\ [2^{\alpha_1-1}, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})] & \alpha_1 \geq 3 \end{cases}$$

5-3 从而有

$$\begin{cases} \text{ord}_m(a) | [1, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})] & \alpha_1 = 0 \\ \text{ord}_m(a) | [1, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})] & \alpha_1 = 1 \\ \text{ord}_m(a) | [2, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})] & \alpha_1 = 2 \\ \text{ord}_m(a) | [2^{\alpha_1-1}, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})] & \alpha_1 \geq 3 \end{cases} \quad \diamond$$

事实上, 设 a 是奇数(比如表示成 $a = 2t + 1, t \in \mathbb{Z}$), 则有 $a^{2^{l-2}} \equiv 1 \pmod{2^l} (l \geq 3)$ 成立, 可以对 l 使用数学归纳法证明这个等式:

当 $l = 3$ 时, $a^2 = 4t(t+1) + 1 \equiv 1 \pmod{2^3}$;

当 $l = n$ 时成立, 即 $a^{2^{n-2}} \equiv 1 \pmod{2^n}$, 即 $a^{2^{n-2}} = k \cdot 2^n + 1$,

当 $l = n + 1$ 时,

$$a^{2^{n-1}} - 1 = (a^{2^{n-2}} - 1)(a^{2^{n-2}} + 1) = k \cdot 2^n (k \cdot 2^n + 2) = k^2 \cdot 2^{2n} + k \cdot 2^{n+1}$$

所以 $a^{2^{n-1}} - 1 \equiv 0 \pmod{2^{n+1}}$, *i.e.*, $a^{2^{n-1}} \equiv 1 \pmod{2^{n+1}}$

这个结论说明, $\text{ord}_{2^l}(a) | 2^{l-2} (l \geq 3)$

所以我们有:

$$[\text{ord}_{2^{\alpha_1}}(a), \text{ord}_{p_2^{\alpha_2}}(a), \dots, \text{ord}_{p_s^{\alpha_s}}(a)] | 2^{\alpha_1-2}, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})$$

即 $\text{ord}_m(a) | 2^{\alpha_1-2}, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})$

5-4 从而有

$$\begin{cases} \text{ord}_m(a)[1, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})] & \alpha_1 = 0 \\ \text{ord}_m(a)[1, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})] & \alpha_1 = 1 \\ \text{ord}_m(a)[2, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})] & \alpha_1 = 2 \\ \text{ord}_m(a)[2^{\alpha_1-2}, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})] & \alpha_1 \geq 3 \end{cases} \quad \diamond$$

重新记右边的最小公倍数为 β , 即

$$m = p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s} : \beta = [1, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})]$$

$$m = 2p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s} : \beta = [1, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})]$$

$$m = 4p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s} : \beta = [2, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})]$$

$$m = 2^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s} : \beta = [2^{\alpha_1-2}, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_s^{\alpha_s})]$$

5-5 模 m 存在原根 $\implies m = 1$, 或 2 , 或 4 , 或 p^α , 或 $2p^\alpha$ (p 是奇素数).

证明: 反设 m 不属于这几种情形, 那么 m 的形式就是 $m = 2^\alpha$ ($\alpha \geq 3$), 或是 $m = 2^\alpha p_1^{\alpha_1} \dots p_r^{\alpha_r}$ ($\alpha \geq 2, r \geq 1$), 或是 $m = 2^\alpha p_1^{\alpha_1} \dots p_r^{\alpha_r}$ ($\alpha \geq 0, r \geq 2$)

< 1 >, 如果 $m = 2^\alpha$ ($\alpha \geq 3$), 则 $\varphi(m) = 2^{\alpha-1}$
但 $\text{ord}_{2^\alpha}(a) | 2^{\alpha-1}$, 所以 $\text{ord}_m(a) \leq 2^{\alpha-2} < 2^{\alpha-1} = \varphi(m)$, 可见这时模 m 没有原根;
< 2 >, 如果 $m = 2^\alpha p_1^{\alpha_1} \dots p_r^{\alpha_r}$ ($\alpha \geq 2, r \geq 1$),
即 $m = 4p_1^{\alpha_1} \dots p_r^{\alpha_r}$ ($r \geq 1$) 或 $m = 2^\alpha p_1^{\alpha_1} \dots p_r^{\alpha_r}$ ($\alpha \geq 3, r \geq 1$), 对应地
有 $\varphi(m) = 2\varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r})$ 和 $\varphi(m) = 2^{\alpha-1}\varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r})$

对应地, 前述的 $\beta = [2, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \dots, \varphi(p_r^{\alpha_r})]$, 注意到 p_i 都是奇素数, 所以 $\varphi(p_i^{\alpha_i}) = p_i^{\alpha_i} - p_i^{\alpha_i-1}$ 都是偶数, 所以 $\beta = [2, \varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}), \dots, \varphi(p_r^{\alpha_r})] = [\varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}), \dots, \varphi(p_r^{\alpha_r})] \leq \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \dots \varphi(p_r^{\alpha_r}) < 2\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \dots \varphi(p_r^{\alpha_r}) = \varphi(m)$, 所以,
 $\forall a, \text{ord}_m(a) < \varphi(m)$, 可见这时模 m 没有原根;
和

$\beta = [2^{\alpha-2}, \varphi(p_1^{\alpha_1}), \varphi(p_2^{\alpha_2}), \dots, \varphi(p_r^{\alpha_r})] \leq 2^{\alpha-2}\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \dots \varphi(p_r^{\alpha_r}) < 2^{\alpha-1}\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2}) \dots \varphi(p_r^{\alpha_r}) = \varphi(m)$,
所以, $\forall a, \text{ord}_m(a) < \varphi(m)$, 可见这时模 m 没有原根;

$< 3 >$, 如果 $m = 2^\alpha p_1^{\alpha_1} \dots p_r^{\alpha_r} (\alpha \geq 0, r \geq 2)$, 即 $m = p_1^{\alpha_1} \dots p_r^{\alpha_r} (r \geq 2)$
 或 $m = 2p_1^{\alpha_1} \dots p_r^{\alpha_r} (r \geq 2)$ 或 $m = 4p_1^{\alpha_1} \dots p_r^{\alpha_r} (\alpha \geq 3, r \geq 2)$ 对应地,

$$\varphi(m) = \varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r})$$

$$\varphi(m) = \varphi(2)\varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) = \varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r})$$

$$\varphi(m) = \varphi(4)\varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) = 2\varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r})$$

$$\varphi(m) = \varphi(2^\alpha)\varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) = 2^{\alpha-1}\varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r})$$

相应的

$$\beta = [1, \varphi(p_1^{\alpha_1}), \dots, \varphi(p_r^{\alpha_r})] < \varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) = \varphi(m)$$

$$\beta = [1, \varphi(p_1^{\alpha_1}), \dots, \varphi(p_r^{\alpha_r})] < \varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) = \varphi(m)$$

$$\beta = [2, \varphi(p_1^{\alpha_1}), \dots, \varphi(p_r^{\alpha_r})] = [\varphi(p_1^{\alpha_1}), \dots, \varphi(p_r^{\alpha_r})] < \varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) <$$

$$2\varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) = \varphi(m)$$

$$\beta = [2^{\alpha-2}, \varphi(p_1^{\alpha_1}), \dots, \varphi(p_r^{\alpha_r})] \leq 2^{\alpha-2}\varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) < 2^{\alpha-1}\varphi(p_1^{\alpha_1}) \dots \varphi(p_r^{\alpha_r}) =$$

$$\varphi(m)$$

所以, $\forall a, \text{ord}_m(a) < \varphi(m)$, 可见这时模 m 没有原根.

可见不论 m 属于反设的哪一种情形, 总有 $\forall a, \text{ord}_m(a) < \varphi(m)$, 所以对 m , 模 m 都没有原根. 所以, 如果模 m 有原根的话, 只能是 1, 或 2, 或 4, 或 p^α , 或是 $2p^\alpha$ \diamond

5-6 $(m, n) = 1$, a_1, a_2 均与 mn 互素, 则存在 a 使得 $\text{ord}_{mn}(a) = [\text{ord}_m(a_1), \text{ord}_n(a_2)]$.

我们知道同余式组 $\begin{cases} x \equiv a_1 \pmod{m} \\ x \equiv a_2 \pmod{n} \end{cases}$ 有唯一解

$$x \equiv [x^{-1} \pmod{m}] \cdot n \cdot a_1 + [m^{-1} \pmod{n}] \cdot m \cdot a_2 \pmod{M}$$

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

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

从而

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

所以我们说: 如果 $a_1 = a_2 \implies \text{ord}_{mn}(a_1) = [\text{ord}_m(a_1), \text{ord}_n(a_1)]$

如果没有条件 $a_1 = a_2$ 的话, 存在 a 使得 $\text{ord}_{mn}(a) = [\text{ord}_m(a_1), \text{ord}_n(a_2)]$

与此对比, 我们知道: $(\text{ord}_m(a), \text{ord}_m(b)) = 1 \implies \text{ord}_m(ab) = [\text{ord}_m(a), \text{ord}_m(b)]$

如果没有条件 $(\text{ord}_m(a), \text{ord}_m(b)) = 1$, 则存在 c , 使得: $\text{ord}_m(c) = [\text{ord}_m(a), \text{ord}_m(b)]$

2. 原根存在的充要条件

定理

设 p 是素数, 则模 p 有原根.

证明: 我们知道存在整数 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 , 我们要说明 $\delta = p-1$, 即这个 g 就是一个模 p 的原根.

对这个 g 肯定有 $g^{p-1} \equiv 1 \pmod p$, 从而 $\delta \leq p-1$.

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

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

所以有 $1^\delta \equiv 1 \pmod p, 2^\delta \equiv 1 \pmod p, \dots, (p-1)^\delta \equiv 1 \pmod p$, 也就是说, 方程

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

至少有 $p-1$ 个解, 从而知道 $\delta \geq p-1$.

从而 $\delta = p-1$, 即这个 g 是模 p 的原根.

定理

设 g 是模 $p^{\alpha+1}$ ($\alpha \geq 1$)的原根, 则 g 必是模 p^α 的原根.

证明: 设 $\text{ord}_{p^\alpha}(g) = \delta$, 从而 $\delta | \varphi(p^\alpha)$,
另外, $g^\delta \equiv 1 \pmod{p^\alpha}$, 即 $g^\alpha = kp^\alpha + 1$,

$$\begin{aligned}(g^\delta)^p &= (kp^\alpha + 1)^p \\&= C_p^0(kp^\alpha)^p + C_p^1(kp^\alpha)^{p-1} + \dots + C_p^{p-2}(kp^\alpha)^2 + C_p^{p-1}(kp^\alpha) + C_p^p 1 \\&= (kp^\alpha)^p + p(kp^\alpha)^{p-1} + \dots + C_p^2(kp^\alpha)^2 + C_p^1(kp^\alpha) + 1 \\&= A \cdot p^{\alpha+1} + kp^{\alpha+1} + 1\end{aligned}$$

$$\therefore (g^\delta)^p \equiv 1 \pmod{p^{\alpha+1}}, \quad \text{i.e., } g^{p\delta} \equiv 1 \pmod{p^{\alpha+1}}$$

从而应该有 $\text{ord}_{p^{\alpha+1}}(g) | p\delta$, i.e., $\varphi(p^{\alpha+1}) | p\delta$, i.e., $p^\alpha(p-1) | p\delta$, 从而 $p^{\alpha-1}(p-1) | p\delta$, 即 $\varphi(p^\alpha) | \delta$.

因此, $\delta = \varphi(p^\alpha)$, 即 g 确实也是模 p^α 的原根. \diamond

注:二项式定理公式: $(a+b)^n = \sum_{i=0}^n C_n^i a^{n-i} b^i$
 $= C_n^0 a^n + C_n^1 a^{n-1} b + C_n^2 a^{n-2} b^2 + C_n^3 a^{n-3} b^3 + \dots + C_n^{n-1} a b^{n-1} + C_n^n b^n$

定理

设 g 是模 p^α 的原根, 则必有 $\text{ord}_{p^{\alpha+1}}(g) = \varphi(p^\alpha)$, 或 $\text{ord}_{p^{\alpha+1}}(g) = \varphi(p^{\alpha+1})$

证明: 由于 $p^\alpha | p^{\alpha+1}$, 由前面指数的性质知:

$$\text{ord}_{p^\alpha}(g) | \text{ord}_{p^{\alpha+1}}(g)$$

所以我们有 $\varphi(p^\alpha) | \text{ord}_{p^{\alpha+1}}(g) = k \cdot \varphi(p^\alpha)$ 另一方面, 我们知道: $\text{ord}_{p^{\alpha+1}} | \varphi(p^{\alpha+1})$, 从而 $\varphi(p^{\alpha+1}) = k' \cdot \text{ord}_{p^{\alpha+1}}(g)$, 从而 $\varphi(p^{\alpha+1}) = k' \cdot k \cdot \varphi(p^\alpha)$

$$\text{即 } p^\alpha(p-1) = kk'p^{\alpha-1}(p-1)$$

从而 $kk' = p$, 即 $k = 1$ 且 $k' = p$, 或者是 $k = p$ 且 $k' = 1$,

所以 $\text{ord}_{p^{\alpha+1}}(g) = \varphi(p^\alpha)$,

或 $\text{ord}_{p^{\alpha+1}}(g) = p\varphi(p^\alpha) = p \cdot p^{\alpha-1}(p-1) = p^\alpha(p-1) = \varphi(p^{\alpha+1})$. \diamond

定理

g 是模奇素数 p 的原根, 且 g 满足 $g^{p-1} = 1 + rp, p \nmid r$, 则 g 是模 $p^\alpha (\forall \alpha \geq 1)$ 的原根.

证明: 我们先来证明对这个原根 g 来说总有:

$$\forall \alpha \geq 1, g^{\varphi(p^\alpha)} = 1 + r_\alpha p^\alpha, p \nmid r_\alpha$$

其中 r_α 是一个整数.

归纳法: $\alpha = 1$ 时就是已知条件;

假设 $\alpha = n$ 时有 $g^{\varphi(p^n)} = 1 + r_n p^n, p \nmid r_n$,

当 $\alpha = n + 1$ 时, 由于 $\varphi(p^{k+1}) = p\varphi(p^k)$, 所以:

$$\begin{aligned} g^{\varphi(p^{n+1})} &= g^{p\varphi(p^n)} = (g^{\varphi(p^n)})^p = (1 + r_n p^n)^p \\ &= 1 + C_p^1 r_n p^n + C_p^2 (r_n p^n)^2 + C_p^3 (r_n p^n)^3 + \dots \\ &= 1 + p^{n+1} r_n + C_p^2 r_n^2 p^{2n} + \dots \\ &= 1 + p^{n+1} [r_n + \dots] \\ &= 1 + r_{n+1} p^{n+1} \end{aligned}$$

由于 $p \nmid r_n$, 所以 $p \nmid r_{n+1}$. 即 $\alpha = n + 1$ 时也成立.

这样, 我们就知道对于满足定理要求的 g 来说有:

$$\begin{aligned} g^{\varphi(p)} &= 1 + r_1 p, p \nmid r_1 & g^{\varphi(p^2)} &= 1 + r_2 p^2, p \nmid r_2 \\ g^{\varphi(p^3)} &= 1 + r_3 p^3, p \nmid r_3 & g^{\varphi(p^4)} &= 1 + r_4 p^4, p \nmid r_4 \quad \dots \end{aligned}$$

由于 g 是模 p 的原根, 由前一定理知道 $\text{ord}_{p^2}(g) = \varphi(p)$ 或 $\varphi(p^2)$,
如果 $\text{ord}_{p^2}(g) = \varphi(p)$ 的话, 则有 $g^{\varphi(p)} \equiv 1 \pmod{p^2}$, 即 $g^{\varphi(p)} = 1 + kp \cdot p$,
与 $g^{\varphi(p)} = 1 + r_1 p (p \nmid r_1)$ 矛盾, 所以 $\text{ord}_{p^2}(g) = \varphi(p^2)$, 即 g 是模 p^2 的原根.

再根据 g 是模 p^2 的原根, $g^{\varphi(p^2)} = 1 + r_3 p^3 (p \nmid r_3)$ 类似可以推出 g 是模 p^3 的原根.

这个过程继续下去可知, 满足定理要求的 g 是模 $p^\alpha (\forall \alpha \geq 1)$ 的原根. \diamond

定理

设 g' 是模奇素数 p 的原根, 则 $g = g', g = g' + p, g = g' + 2p, \dots, g = g' + (p-1)p$ 都是模 p 的原根.

这是显然的, 因为对于 $g = g' + tp, t = 0, 1, \dots, p-1$, 有 $g \equiv g' \pmod{p}$
所以有 $\forall i \geq 1: g^i \equiv g'^i \pmod{p}$,
而 g' 是模 p 的原根, 即

$$g'^i \not\equiv 1 \pmod{p}, (i < p-1)$$

$$g'^{p-1} \equiv 1 \pmod{p}$$

从而

$$g^i \not\equiv 1 \pmod{p} (i < p-1)$$

$$g^{p-1} \equiv 1 \pmod{p}$$

即 g 也是模 p 的原根.. \diamond

另外我们也可以看到, 在这 p 个 g 中, 除了一个外, 其他的 g 都满足: $g^{p-1} = 1 + rp, p \nmid r$.

事实上, 注意到

$$g^{p-1} = (g' + tp)^{p-1} = g'^{p-1} + (p-1)g'^{p-2}(tp) + Ap^2$$

其中 A 是一个整数. 由于 g' 是模 p 的原根, 可设 $g'^{p-1} = 1 + ap$, 从而

$$g^{p-1} = 1 + [(p-1)g'^{p-2}t + a]p + Ap^2 = 1 + [(p-1)g'^{p-2}t + (a + Ap)]p$$

又由于 $(p, p-1) = 1$, $(p, g') = 1$, 所以 $(p, (p-1)g') = 1$, $(p, (p-1)g'^2) = 1$,
 $(p, (p-1)g'^3) = 1, \dots, (p, (p-1)g'^{p-2}) = 1$,

所以关于 t 的一次同余方程 $(p-1)g'^{p-2}t + (a + Ap) \equiv 0 \pmod{p}$ 有唯一解.
这也就是说 p 个 g 中只有一个不满足条件 $g^{p-1} = 1 + rp, p \nmid r$, 其余都满足.

这样我们就可以说: 设 p 是奇素数, g' 为模 p 的原根,

则 $g = g', g = g' + p, g = g' + 2p, \dots, g = g' + (p-1)p$ 都是模 p 的原根, 且只有一个不满足条件 $g^{p-1} = 1 + rp, p \nmid r$, 其余都满足.

在这个结论中, 如果我们还要求 g' 满足条件“ g' 为奇数”, 则由于 $t = 0, 1, 2, \dots, p-1$ 中至少有2个偶数, 从而 $g = g' + tp (t = 0, 1, \dots, p-1)$ 中至少有两个是奇数, 所以这两个中(从而这 p 个 g 中)必定存在一个满足: (i)是奇数;(ii)是模 p 的原根;(iii)满足条件 $g^{p-1} = 1 + rp, p \nmid r$.

如果原根 g' 不是奇数(即是偶数), 则令 $g'' := g' + p$, 则 g'' 是一个为奇数的模 p 的原根, 用这个 g'' 来构造 g 即可.

综上, 我们总可以有任意的模 p 的原根 g' , 构造一个为奇数的模 p 的原根 \tilde{g} 满足 $\tilde{g}^{p-1} = 1 + rp, p \nmid r$.

找到的这个 \tilde{g} 自然也是模 $p^\alpha (\forall \alpha \geq 1)$ 的原根.

由于 \tilde{g} 是奇数, 所以我们可以知道

$$\tilde{g}^d \equiv 1 \pmod{p^\alpha} \iff \tilde{g}^d \equiv 1 \pmod{2p^\alpha}$$

事实上, 如果 $\tilde{g}^d \equiv 1 \pmod{2p^\alpha}$, 则显然有 $\tilde{g}^d \equiv 1 \pmod{p^\alpha}$;

反之, 如果 $\tilde{g}^d \equiv 1 \pmod{p^\alpha}$, 即 $p^\alpha | \tilde{g}^d - 1$, 而 $2 | \tilde{g}^d - 1$, 且 $(2, p) = 1$, 所以 $[2, p^\alpha] = 2p^\alpha$, 且 $2p^\alpha | \tilde{g}^d - 1$, 即 $\tilde{g}^d \equiv 1 \pmod{2p^\alpha}$.

这样,我们就知道

$$\text{ord}_{p^\alpha}(\tilde{g}) = \text{ord}_{2p^\alpha}(\tilde{g})$$

$$\therefore \text{ord}_{2p^\alpha}(\tilde{g}) = \varphi(p^\alpha)$$

$$\because \varphi(2p^\alpha) = \varphi(p^\alpha)$$

$$\therefore \text{ord}_{2p^\alpha}(\tilde{g}) = \varphi(2p^\alpha)$$

即找到的这个 \tilde{g} 也是模 $2p^\alpha$ 的原根.

整理我们得到的结论:

- ① p 为奇素数, 模 p 的原根必存在, 比如说是 g' ;
- ② 有这个模 p 的原根 g' 可以构造出一个模 p 的原根 \tilde{g} 满足:
是奇数, 且 $\tilde{g}^{p-1} = 1 + rp (p \nmid r)$;
- ③ 这个模 p 的原根 \tilde{g} 也是模 p^α 的原根;
- ④ 这个模 p 的原根 \tilde{g} 也是模 $2p^\alpha$ 的原根;

上述几点说明:

一方面模 p 的原根必定存在, 模 p^α 的原根必定存在, 模 $2p^\alpha$ 的原根必定存在;

另一方面, 只要知道了模 p 的任意一个原根, 就可以计算出来模 p^α 的原根和模 $2p^\alpha$ 的原根.

定理

模 m 有原根的充要条件是 $m = 1$,或 2 ,或 4 ,或 p^α ,或 $2p^\alpha$.

在指数的性质中, 我们已经证明了模 m 有原根的必要条件:

模 m 有原根 $\implies m = 1$,或 2 ,或 4 ,或 p^α ,或 $2p^\alpha$

所以,下面我们需要证明模 m 有原根的充分条件:

$m = 1$,或 2 ,或 4 ,或 p^α ,或 $2p^\alpha \implies$ 模 m 有原根.

事实上, 很容易检查:

- 如果 $m = 1$ 的话, 模1的原根就是1: $\varphi(m) = 1, 1^1 = 1$;
- 如果 $m = 2$ 的话, 模2的原根就是1: $\varphi(m) = 1, 1^1 = 1$;
- 如果 $m = 4$ 的话, 模4的原根就是3: $\varphi(m) = 2, 3^1 = 3, 3^2 = 9 \equiv 1 \pmod{4}$;
- 前面业已说明 $m = p^\alpha$ 时, 模 m 有原根; $m = 2p^\alpha$ 时, 模 m 有原根.



说明: 上述求模 m 的原根问题最终归结为求模 p 的原根问题.

但是求模 p 的原根没有统一的方法, 只能对具体的素数 p 按照原根的定义逐个数去试.

示例: 求模 $p = 23$ 的原根.

由于 $\forall a$ 对模 p 的指数必定是 $p - 1$ 的因子,

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.

3. 指标

我们前面看到, 当 g 是模 m 的原根时(即 g 与模 m 互素, $\text{ord}_m(g) = \varphi(m)$), $g^1, g^2, \dots, g^{\varphi(m)-1}, g^{\varphi(m)}$ 两两模 m 不同余, 它们构成了一个模 m 的简化剩余系: $\{g^1, g^2, \dots, g^{\varphi(m)-1}, g^{\varphi(m)}\}$.

换句话说, 对于任意的与 m 互素的整数 a (即 a 是模 m 的一个简化剩余)来说, 在 $1 \sim \varphi(m)$ 之间存在唯一一个数 r , 使得 $g^r \equiv a \pmod{m}$, 我们就把这个数 r 称为以 g 为底的 a 对模 m 的指标, 记作 $\text{ind}_g a$, 或 inda (注意到此时 g 必须为模 m 的原根)

比如, $g = 5$ 是模 $m = 17$ 的一个原根, 且

| 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 |

所以以5为底9对模17的指标就是10, 以5为底4对模17的指标就是12...

定理

$$g^s \equiv a \pmod{m} \implies s \equiv \text{ind}_g a \pmod{\varphi(m)}$$

事实上,

$$\begin{aligned}\because g^s &\equiv a \pmod{m} \\ g^{\text{ind}_g a} &\equiv a \pmod{m} \\ \therefore g^s &\equiv g^{\text{ind}_g a} \pmod{m}\end{aligned}$$

不妨设 $\text{ind}_g a \leq s$ 由于 $(g, m) = 1$,

$$\therefore g^{s - \text{ind}_g a} \equiv 1 \pmod{m}$$

另外, 由于 g 是原根, 所以 g 的指数是 $\varphi(m)$, 从而 $\varphi(m) | (s - \text{ind}_g a)$,
即 $s \equiv \text{ind}_g a \pmod{\varphi(m)}$ \diamond

示例: 已知6是模41的原根, 以6为底的9对模41的指标为30, 即 $\text{ind}_6 9 = 30$, 求 $x^5 \equiv 9 \pmod{41}$ 的解:

设 x_1 是这个方程的解, 则有 $x_1^5 \equiv 9 \pmod{41}$
即 x_1^5 与9在同一个模41的剩余类中, 而9与41互素, 所以 x_1^5 与41互素, 从而 x_1 与41互素.

因为6是模41的原根, 所以可设 $x_1 = 6^{y_1} \pmod{41}$, 则 $x_1^5 \equiv 9 \pmod{41}$ 就等价于 $6^{5y_1} \equiv 9 \pmod{41}$, 从而

$$5y_1 \equiv \text{ind}_6 9 \pmod{40} (\because g^s \equiv a \pmod{m} \implies s \equiv \text{ind}_g a \pmod{\varphi(m)})$$

即

$$5y_1 \equiv 30 \pmod{40}, \quad i.e., \quad y_1 \equiv 6, 14, 22, 30, 38 \pmod{40}$$

对应的有

$$x \equiv 6^6 \pmod{41}, x \equiv 6^{14} \pmod{41}, \dots \quad \diamond$$

定理

g 为模 m 的原根, a_1, \dots, a_n 均与 m 互素, 则

$$\text{ind}_g(a_1 \dots a_n) \equiv \text{ind}_g a_1 + \dots + \text{ind}_g a_n \pmod{\varphi(m)}$$

事实上,

$$\left. \begin{array}{l} g^{\text{ind}_g(a_1)} \equiv a_1 \pmod{m} \\ g^{\text{ind}_g(a_2)} \equiv a_2 \pmod{m} \\ \dots\dots\dots \\ g^{\text{ind}_g(a_n)} \equiv a_n \pmod{m} \end{array} \right\} \Rightarrow (a_1 a_2 \dots a_n) \equiv g^{\text{ind}_g(a_1)} g^{\text{ind}_g(a_2)} \dots g^{\text{ind}_g(a_n)} \pmod{m}$$

$$\Rightarrow (a_1 a_2 \dots a_n) \equiv g^{\text{ind}_g(a_1) + \text{ind}_g(a_2) + \dots + \text{ind}_g(a_n)} \pmod{m}$$

$$\Rightarrow \text{ind}_g(a_1) + \text{ind}_g(a_2) + \dots + \text{ind}_g(a_n) \equiv \text{ind}_g(a_1 a_2 \dots a_n) \pmod{\varphi(m)} \quad \diamond$$

指数与指标间的联系:

假设 g 为模 m 的原根, a 与 m 互素, 其指标记为 $\text{ind}_g a$, a 的指数记作 $\text{ord}_m(a)$, 则:
事实上, 我们知道 $g^{\text{ind}_g a} \equiv a \pmod{m}$,

$$\begin{aligned}\text{ord}_m(a) &= \text{ord}_m(g^{\text{ind}_g a}) (\because r \equiv s \pmod{m} \implies \text{ord}_m r = \text{ord}_m s) \\ &= \frac{\text{ord}_m(g)}{(\text{ord}_m(g), \text{ind}_g a)} \\ &= \frac{\varphi(m)}{(\varphi(m), \text{ind}_g a)} \\ &\quad \text{i.e., } \varphi(m) = (\varphi(m), \text{ind}_g a) \cdot \text{ord}_m(a)\end{aligned}$$

由此可见,

定理

a 是模 m 的原根 $\iff (\varphi(m), \text{ind}_g a) = 1$

定理

在模 m 的简化剩余系中, 指数等于 e 的整数个数是 $\varphi(e)$.

假设 a 与 m 互素(即在一个简化剩余系中), 则

$$\text{ord}_m(a) = \frac{\varphi(m)}{(\varphi(m), \text{ind}_g a)}$$

记 $i = \text{ind}_g a$ (从而 $1 \leq i \leq \varphi(m)$), 则有

$$e = \text{ord}_m(a) \iff e = \frac{\varphi(m)}{(\varphi(m), i)}$$

这样指数等于 e 的 a 的个数就是使得 $e = \frac{\varphi(m)}{(\varphi(m), i)}$ 成立的 i 的个数, 所以只需讨论式子

$$e = \frac{\varphi(m)}{(\varphi(m), i)} \iff (\varphi(m), i) = \frac{\varphi(m)}{e} \iff \left(\frac{i}{\frac{\varphi(m)}{e}}, \frac{\varphi(m)}{e} \right) = 1$$

$$\text{i.e., } (i', e) = 1 (0 \leq i' \leq e)$$

这样使得 $e = \frac{\varphi(m)}{(\varphi(m), i)}$ 成立的 i 的个数就是使得 $(i', e) = 1 (0 \leq i' \leq e)$ 的 i' 的个数, 即 $\varphi(e)$. \diamond

根据这个结论, 模 m 的简化剩余系中指数为 $\varphi(m)$ 的整数(即原根)的个数就是 $\varphi(\varphi(m))$.

4. n 次剩余

$m > 1$, a 与 m 互素, 如果同余式 $x^n \equiv a \pmod{m}$ 有解, 则称 a 为模 m 的 n 次剩余.
否则, 称为模 m 的 n 次非剩余.

定理

设 g 是模 m 的一个原根, a 与 m 互素, 则 $x^n \equiv a \pmod{m}$ 有解 $\iff (n, \varphi(m)) \mid \text{ind}_g a$.
如果有解的话, 解数为 $(n, \varphi(m))$.

证明: " \implies :" 设同余式有解: $x \equiv x_0 \pmod{m}$, 即 $x_0^n \equiv a \pmod{m}$, 也就是说 x_0^n 与 a 在同一个模 m 剩余类中,

而 a 与 m 互素, 所以 x_0^n 也与 m 互素,
从而 x_0 也与 m 互素, 即 x_0 是模 m 的一个简化剩余,

这样就存在一个整数 u 使得 $x_0 \equiv g^u \pmod{m}$,

从而 $g^{un} \equiv a \pmod{m}$, 从而 $un \equiv \text{ind}_g a \pmod{\varphi(m)}$

也就是说, $ny \equiv \text{ind}_g a \pmod{\varphi(m)}$ 有解,

从而应该 $(n, \varphi(m)) \mid \text{ind}_g a$.

" \impliedby :" 如果 $(n, \varphi(m)) \mid \text{ind}_g a$, 则一次同余式 $ny \equiv \text{ind}_g a \pmod{\varphi(m)}$ 有解, 且解数为 $(n, \varphi(m))$,

比如说 $y \equiv u \pmod{\varphi(m)}$ 是一个解, 则 $nu \equiv \text{ind}_g a \pmod{\varphi(m)}$, 即 $nu = k\varphi(m) + \text{ind}_g a$,
从而 $(g^u)^n = g^{un} = g^{k\varphi(m) + \text{ind}_g a} = g^{k\varphi(m)} g^{\text{ind}_g a} \equiv a \pmod{m}$, 即 $x \equiv y^u \pmod{m}$ 就是原 n 次同余方程的一个解. \diamond

令 $d = (n, \varphi(m))$,

由前我们看到, $x^n \equiv a \pmod{m}$ 有解 $\iff (n, \varphi(m)) \mid \text{ind}_g a$

下面来说明

$$(n, \varphi(m)) \mid \text{ind}_g a \iff \exists s \in \mathbb{Z}, \text{ s.t.}, \frac{\varphi(m)}{(n, \varphi(m))} = s \cdot \text{ord}_m(a)$$

注意到我们总有结论 $\varphi(m) = (\varphi(m), \text{ind}_g a) \cdot \text{ord}_m(a)$ 可以使用.

" \implies :" 已知 $(n, \varphi(m)) \mid \text{ind}_g a$, 即 $d \mid \text{ind}_g a$

设 $n = k_n d, \varphi(m) = k d, \text{ind}_g a = k_i d$, 则

$$\begin{aligned} \frac{\varphi(m)}{(n, \varphi(m))} &= \frac{(\varphi(m), \text{ind}_g a) \cdot \text{ord}_m(a)}{d} \\ &= \frac{(k d, k_i d) \cdot \text{ord}_m(a)}{d} \\ &= \frac{(k, k_i) d \cdot \text{ord}_m(a)}{d} = (k, k_i) \cdot \text{ord}_m(a) \end{aligned}$$

s 已找到.

" \Leftarrow :" 反过来, 已知

$$\exists s \in \mathbb{Z}, s.t., \frac{\varphi(m)}{(n, \varphi(m))} = s \cdot \text{ord}_m(a)$$

要证 $d | \text{ind}_g a$. 设 $\varphi(m) = kd$, 由

$$\frac{\varphi(m)}{(n, \varphi(m))} = s \cdot \text{ord}_m(a)$$

知

$$k = s \cdot \text{ord}_m(a) \quad (1.1)$$

又由 $\varphi(m) = (\varphi(m), \text{ind}_g a) \cdot \text{ord}_m(a)$ 知

$$kd = (\varphi(m), \text{ind}_g a) \cdot \text{ord}_m(a) \quad (1.2)$$

将(1.1)代入(1.2)知

$$(\varphi(m), \text{ind}_g a) = sd$$

从而

$$d | \text{ind}_g a \quad \diamond$$

至此,我们证明了

$$(n, \varphi(m)) | \text{ind}_g a \iff \exists s \in \mathbb{Z}, s.t., \frac{\varphi(m)}{(n, \varphi(m))} = s \cdot \text{ord}_m(a)$$

即

$$(n, \varphi(m)) | \text{ind}_g a \iff \text{ord}_m(a) | \frac{\varphi(m)}{(n, \varphi(m))}$$

从而我们可以说:

$$\begin{aligned} x^n \equiv a \pmod{m} \text{ 有解} &\iff (n, \varphi(m)) | \text{ind}_g a \\ &\iff \text{ord}_m(a) | \frac{\varphi(m)}{(n, \varphi(m))} \\ &\iff a^{\frac{\varphi(m)}{(n, \varphi(m))}} \equiv 1 \pmod{m} \end{aligned}$$

这样我们就有结论: 模 m 原根存在, 则

$$a \text{ 是模 } m \text{ 的 } n \text{ 次剩余} \iff a^{\frac{\varphi(m)}{(n, \varphi(m))}} \equiv 1 \pmod{m}. \quad \diamond$$

