# 阶 & 原根

前置知识：费马小定理、欧拉定理、拉格朗日定理

阶和原根，是理解模 $m$ 既约剩余系 $\mathbf{Z}_m^*$ 乘法结构的重要工具．基于此，可以定义 离散对数 等概念．更为一般的讨论可以参见抽象代数部分 群论 和 环论 等页面相关章节．

## 阶

本节中，总是假设模数 $m \in \mathbf{N}_+$ 和底数 $a \in \mathbf{Z}$ 互素，即 $(a, m) = 1$，也记作 $a \perp m$．

对于 $n \in \mathbf{Z}$，幂次 $a^n \bmod m$ 呈现一种循环结构．这个循环节的最小长度，就是 $a$ 模 $m$ 的阶．阶就定义为幂 $a^n \bmod m$ 第一次回到起点 $a^0 \bmod m = 1$ 时的指数：

**阶**

$a \in \mathbf{Z}, m \in \mathbf{N}_+$　$a \perp m$　$a^n \equiv 1 \pmod{m}$　$n$　**$a$ 模 $m$ 的阶**

$a$　$m$　$\delta_m(a)$　$\operatorname{ord}_m(a)$

**注**

$m$　$a$　$\delta$

$\delta^-$　$a^n \equiv -1 \pmod{m}$

### 幂的循环结构

利用阶，可以刻画幂的循环结构．对于幂 $a^n \bmod m$，可以将指数 $n$ 对阶 $\delta_m(a)$ 做带余除法：

$$n = \delta_m(a)q + r,\ 0 \le r < \delta_m(a).$$

进而，利用幂的运算律，就得到

$$a^n = a^{\delta_m(a)q+r} = (a^{\delta_m(a)})^q \cdot a^r \equiv a^r \pmod{m}.$$

这说明，对于任意指数的幂，可以将它平移到第一个非负的循环节．由此，可以得到一系列关于阶的性质．

**性质 1**

$a \in \mathbf{Z}, m \in \mathbf{N}_+$ $a \perp m$ $a^0(=1), a, a^2, \cdots, a^{\delta_m(a)-1}$ $m$

**证明**

$0 \le i < j < \delta_m(a)$ $a^i \equiv a^j \pmod{m}$ $a^{j-i} \equiv 1 \pmod{m}$ $0 < j - i < \delta_m(a)$

**性质 2**

$a, n \in \mathbf{Z}, m \in \mathbf{N}_+$ $a \perp m$ $a^n \equiv 1 \pmod{m}$ $\delta_m(a) \mid n$

**证明**

$a^n \equiv a^{n \bmod \delta_m(a)} \pmod{m}$ $0 \le r < \delta_m(a)$ $a^r \equiv 1 \pmod{m}$ $r$ $r = 0$ $a^n \equiv 1 \pmod{m}$ $n \bmod \delta_m(a) = 0$ $\delta_m(a) \mid a$

欧拉定理 中，同余关系 $a^{\varphi(m)} \equiv 1 \pmod{m}$ 对于所有 $a \perp m$ 都成立．结合性质 2，这说明对于所有 $a \perp m$，都有 $\delta_m(a) \mid \varphi(m)$．换句话说，$\varphi(m)$ 是所有 $a \perp m$ 的阶的一个公倍数．对于一个正整数 $m$，所有 $a \perp m$ 的阶 $\delta_m(a)$ 的最小公倍数，记作 $\lambda(m)$，就是 $m$ 的 Carmichael 函数．后文会详细讨论它的性质．

和其他的循环结构类似，可以根据 $a$ 的阶计算 $a^k$ 的阶．

**性质 3**

$k, a \in \mathbf{Z}, m \in \mathbf{N}_+$ $a \perp m$

$$\delta_m(a^k) = \frac{\delta_m(a)}{(\delta_m(a), k)}.$$

**证明**

$$(a^k)^n = a^{kn} \equiv 1 \pmod{m} \qquad \delta_m(a) \mid kn$$

$$\frac{\delta_m(a)}{(\delta_m(a), k)} \mid n.$$

$$\delta_m(a^k) = \frac{\delta_m(a)}{(\delta_m(a), k)}.$$

## 乘积的阶

设 $a, b$ 是与 $m$ 互素的不同整数．如果已知阶 $\delta_m(a)$ 和 $\delta_m(b)$，那么，同样可以获得一些关于它们乘积 $ab$ 的阶 $\delta_m(ab)$ 的信息．

**性质 4**

$$a, b \in \mathbf{Z}, m \in \mathbf{N}_+ \qquad a, b \perp m$$

$$\frac{[\delta_m(a), \delta_m(b)]}{(\delta_m(a), \delta_m(b))} \mid \delta_m(ab) \mid [\delta_m(a), \delta_m(b)].$$

**证明**

$[\delta_m(a), \delta_m(b)]$ $\delta_m(a)$ $\delta_m(b)$

$$(ab)^{[\delta_m(a),\delta_m(b)]} = a^{[\delta_m(a),\delta_m(b)]} b^{[\delta_m(a),\delta_m(b)]} \equiv 1 \pmod{m}.$$

$$\delta_m(ab) \mid [\delta_m(a), \delta_m(b)].$$

$$1 \equiv (ab)^{\delta_m(ab)\delta_m(b)} \equiv a^{\delta_m(ab)\delta_m(b)} \pmod{m},$$

$\delta_m(a) \mid \delta_m(ab)\delta_m(b)$ $(\delta_m(a), \delta_m(b))$

$$\frac{\delta_m(a)}{(\delta_m(a), \delta_m(b))} \mid \delta_m(ab) \frac{\delta_m(b)}{(\delta_m(a), \delta_m(b))}.$$

$$\frac{\delta_m(a)}{(\delta_m(a), \delta_m(b))} \mid \delta_m(ab).$$

$$\frac{\delta_m(b)}{(\delta_m(a), \delta_m(b))} \mid \delta_m(ab).$$

$$\frac{[\delta_m(a), \delta_m(b)]}{(\delta_m(a), \delta_m(b))} = \frac{\delta_m(a)\delta_m(b)}{(\delta_m(a), \delta_m(b))^2} \mid \delta_m(ab).$$

对于 $a$ 和 $b$ 的阶互素的情形，这一结论有着更为简单的形式.

**性质 4'**

$a, b \in \mathbf{Z}, m \in \mathbf{N}_+$ $a, b \perp m$

$$\delta_m(ab) = \delta_m(a)\delta_m(b) \iff \delta_m(a) \perp \delta_m(b).$$

**证明**

$\delta_m(a) \perp \delta_m(b)$

$$\delta_m(ab) = [\delta_m(a), \delta_m(b)] = \delta_m(a)\delta_m(b).$$

$\delta_m(ab) = \delta_m(a)\delta_m(b)$

$$\delta_m(a)\delta_m(b) = \delta_m(ab) \mid [\delta_m(a), \delta_m(b)].$$

$(\delta_m(a), \delta_m(b)) = 1$ $\delta_m(a) \perp \delta_m(b)$

一般情形中，性质 4 得到的界已经是紧的．乘积的阶取得下界的情形很容易构造：例如 $(a, b, m) = (3, 5, 7)$ 时，$\delta_m(a) = \delta_m(b) = 6$，但是它们的乘积的阶 $\delta_m(ab) = 1$．

尽管一般情形中，乘积 $ab$ 的阶未必是它们的阶的最小公倍数，但是总能找到一个元素使得它的阶等于这个最小公倍数．

**性质 5**

$a, b \in \mathbf{Z}, m \in \mathbf{N}_+$ $a, b \perp m$ $c \in \mathbf{Z}$ $c \perp m$

$$\delta_m(c) = [\delta_m(a), \delta_m(b)].$$

**证明**

$$\delta_m(a) = \prod_p p^{\alpha_p},\ \delta_m(b) = \prod_p p^{\beta_p}.$$

$\alpha_p$ $\beta_p$

$$A = \{p : \alpha_p \geq \beta_p\},\ B = \{p : \alpha_p < \beta_p\}.$$

$$\gamma_A = \prod_{p\in A} p^{\alpha_p},\ \gamma_B = \prod_{p\in B} p^{\alpha_p},\ \eta_A = \prod_{p\in A} p^{\beta_p},\ \eta_B = \prod_{p\in B} p^{\beta_p},$$

$\delta_m(a) = \gamma_A\gamma_B$ $\delta_m(b) = \eta_A\eta_B$

$$\delta_m(a^{\gamma_B}) = \frac{\delta_m(a)}{(\delta_m(a), \gamma_B)} = \frac{\delta_m(a)}{\gamma_B} = \gamma_A,$$
$$\delta_m(b^{\eta_A}) = \frac{\delta_m(b)}{(\delta_m(b), \eta_A)} = \frac{\delta_m(b)}{\eta_A} = \eta_B.$$

$\gamma_A \perp \eta_B$

$$\delta_m(a^{\gamma_B}b^{\eta_A}) = \gamma_A\eta_B = \prod_p p^{\max\{\alpha_p,\beta_p\}} = [\delta_m(a), \delta_m(b)].$$

$c = a^{\gamma_B}b^{\eta_A}$ $[\delta_m(a), \delta_m(b)]$

这一结论常用于构造出指定阶的元素.

## 原根

原根是一些特殊元素——它的阶就等于所有模 $m$ 既约剩余系的个数.

**原根**

$m \in \mathbf{N}_+$ $g \in \mathbf{Z}$ $g \perp m$ $\delta_m(g) = |\mathbf{Z}_m^*| = \varphi(m)$ $g$ **模 $m$ 的原根**
$m$ $\varphi(m)$

并非所有正整数 $m$ 都存在模 $m$ 的原根. 由上文的性质 1，如果模 $m$ 的原根 $g$ 存在，那么，$g, g^2, \cdots, g^{\varphi(m)}$ 所在的同余类互不相同，构成模 $m$ 既约剩余系. 特别地，对于素数 $p$，余数 $g^i \bmod p$ 对于 $i = 1, 2, \cdots, p-1$ 两两不同.

**注**

$m$

$m$

模为 1 时，模 1 整数乘法群就是 $\{0\}$．这显然是循环群，所以原根就是 0．

## 原根判定定理

如果已知模数 $\varphi(m)$ 的全体素因子，那么很容易判断模 $m$ 的原根是否存在．

**定理**

$m \geq 3$ $g \perp m$ $g$ $m$ $\varphi(m)$ $p$

$$g^{\frac{\varphi(m)}{p}} \not\equiv 1 \pmod{m}.$$

**证明**

$g$ $m$

$\delta_m(g) < \varphi(m)$ $\delta_m(g) \mid \varphi(m)$ $p$ $\frac{\varphi(m)}{\delta_m(g)}$

$\delta_m(g) \mid \frac{\varphi(m)}{p}$

$$g^{\frac{\varphi(m)}{p}} \equiv 1 \pmod{m}.$$

$p$ $\varphi(m)$

## 原根个数

原根如果存在，也未必唯一．一般地，对于模 $m$ 既约剩余系中所有元素可能的阶和某个阶的元素数量，有如下结论：

**定理**

$m$ $g$ $d \mid \varphi(m)$ $m$ $d$ $\varphi(d)$

$m$ $\varphi(\varphi(m))$

**证明**

$m$ $g^k \bmod m$ $k$ $1, 2, \cdots, \varphi(m)$

$$\delta_m(g^k) = \frac{\varphi(m)}{(\varphi(m), k)}.$$

$d$ $d \mid \varphi(m)$ $d \mid \varphi(m)$ $d' = \varphi(m)/d$

$$\begin{aligned} A &= \{g^k : (\varphi(m), k) = d',\ 1 \le k \le \varphi(m)\} \\ &= \{g^k : d' \mid k,\ (d, k/d') = 1,\ 1 \le k/d' \le d\}. \end{aligned}$$

$k' = k/d'$ $d$ $d$

$\varphi(d)$

## 原根存在定理

本节将建立如下原根存在定理：

**定理**

$m$ $m = 1, 2, 4, p^e, 2p^e$ $p$ $e \in \mathbf{N}_+$

为说明这一结论，需要分别讨论如下四种情形：

1. $m = 1, 2, 4$，原根分别是 $g = 0, 1, 3$，显然存在．
2. $m = p^e$ 是奇素数的幂，其中，$p$ 为奇素数，$e \in \mathbf{N}_+$．

**引理 1**

$p$ $p$

**证明**

**第一步** $d \mid (p-1)$ $x^d \equiv 1 \pmod{p}$ $d$

$p-1=kd$

$$f(x)=x^{d(k-1)}+x^{d(k-2)}+\cdots+x^d+1.$$

$(x^d-1)f(x)=x^{p-1}-1\equiv 0 \pmod{p}$ $p-1$

$x^d-1$ $f(x)$ $d$

$d(k-1)$ $d+d(k-1)=p-1$ $d$

$x^d \equiv 1 \pmod{p}$ $d$

**第二步** $d \mid (p-1)$ $d$ $\varphi(d)$

$\varphi(m)$ $1$ $1$

$d \mid (p-1)$ $x^d \equiv 1 \pmod{m}$

$\delta_p(x) \mid d$ $d$

$$N(d)=d-\sum_{e\mid d,\, e\neq d} N(e)=d-\sum_{e\mid d,\, e\neq d}\varphi(e)=\varphi(d).$$

$d \mid (p-1)$ $\varphi(d)$ $d$

$d=p-1$ $\varphi(p-1)$ $(p-1)$ $p$

**引理 2**

$p$ $e \in \mathbf{N}_+$ $p^e$

**证明**

**第一步** $p$ $g$ $g^{p-1} \not\equiv 1 \pmod{p^2}$

$p$ $g$ $g^{p-1} \equiv 1 \pmod{p^2}$ $g+p$
$g+p$ $p$

$$\begin{aligned}(g+p)^{p-1} &\equiv \binom{p-1}{0} g^{p-1} + \binom{p-1}{1} g^{p-2} p \\ &= g^{p-1} + g^{p-2} p(p-1) \\ &\equiv 1 - p g^{p-2} \not\equiv 1 \pmod{p^2}.\end{aligned}$$

**第二步** $g$ $e \geq 1$ $g^{\varphi(p^e)} \not\equiv 1 \pmod{p^{e+1}}$

$g$ $e=1$ $e$ $e+1$
$e \geq 1$ $\lambda$

$$g^{\varphi(p^e)} = 1 + \lambda p^e$$

$\lambda \perp p$ $\varphi(p^{e+1}) = p\varphi(p^e)$

$$g^{\varphi(p^{e+1})} = \left(g^{\varphi(p^e)}\right)^p = (1+\lambda p^e)^p \equiv 1 + \lambda p^{e+1} \pmod{p^{e+2}}.$$

$\lambda \perp p$ $g^{\varphi(p^{e+1})} \not\equiv 1 \pmod{p^{e+2}}$

**第三步** $g$ $e \geq 1$ $p^e$

$g$ $e=1$ $e$ $e+1$
$\delta_{p^{e+1}}(g)$ $\delta$ $g^\delta \equiv 1 \pmod{p^{e+1}}$ $g^\delta \equiv 1 \pmod{p^e}$
$\delta_{p^e}(g) = \varphi(p^e)$ $\varphi(p^e) \mid \delta$
$\delta \mid \varphi(p^{e+1})$ $\varphi(p^{e+1}) = p\varphi(p^e)$ $\delta = \varphi(p^e)$ $\delta = \varphi(p^{e+1})$
$g^{\varphi(p^e)} \not\equiv 1 \pmod{p^{e+1}}$ $\delta = \varphi(p^e)$
$\delta = \varphi(p^{e+1})$ $g$ $p^{e+1}$ $e \geq 1$

3. $m = 2p^e$，其中，$p$ 为奇素数，$e \in \mathbf{N}_+$.

**引理 3**

$p$ $e \in \mathbf{N}_+$ $2p^e$

**证明**

$g$ $p^e$ $g+p^e$ $p^e$
$g$ $(g, 2p^e) = 1$ $\delta = \delta_{2p^e}(g)$ $\delta = \varphi(2p^e)$ $\delta \mid \varphi(2p^e)$
$g^\delta \equiv 1 \pmod{2p^e}$ $g^\delta \equiv 1 \pmod{p^e}$ $g$
$\delta_{p^e}(g) = \varphi(p^e) \mid \delta$ $\varphi(2p^e) = \varphi(p^e)$
$\delta = \delta_{2p^e}(g) = \varphi(p^e)$ $\delta$ $2p^e$

4. $m \neq 1, 2, 4, p^e, 2p^e$，其中，$p$ 为奇素数，$e \in \mathbf{N}_+$.

**引理 4**

$m \neq 1, 2, 4$ $p$ $e$ $m = p^e$ $m = 2p^e$ $m$

**证明**

$m = 2^e$ $e \geq 3$ $m$ $g$ $g \perp m$
$g = 2k + 1$ $k \in \mathbf{N}$

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

$k$ $(2^{e-2} - 1)k^2$
$\delta_{2^e}(g) \leq 2^{e-2} < \varphi(2^e) = 2^{e-1}$ $g$

$m$ $2$ $2 < m_1 < m_2$ $m_1 \perp m_2$
$m = m_1 m_2$ $m$ $g$ $g \perp m$ $i = 1, 2$ $g \perp m_i$

$$g^{\varphi(m_i)} \equiv 1 \pmod{m_i}.$$

$m_i > 2$ $\varphi(m_i)$ $i = 1, 2$

$$g^{\frac{1}{2}\varphi(m_1)\varphi(m_2)} \equiv 1 \pmod{m_i}.$$

$$g^{\frac{1}{2}\varphi(m_1)\varphi(m_2)} \equiv 1 \pmod{m}.$$

$\varphi(m) = \varphi(m_1)\varphi(m_2)$

$$\delta_m(g) \leq \frac{1}{2}\varphi(m_1)\varphi(m_2) = \frac{1}{2}\varphi(m) < \varphi(m).$$

$g$ $m$ $m$

综合以上四个引理，我们便给出了一个数存在原根的充要条件.

## 最小原根的范围估计

王元[1]和 Burgess[2]证明了素数 $p$ 的最小原根 $g_p = O\left(p^{0.25+\epsilon}\right)$，其中 $\epsilon > 0$．Cohen, Odoni, and Stothers[3]和 Elliott and Murata[4]分别证明了该估计对于模数 $p^2$ 和 $2p^2$ 也成立，其中，$p$ 是奇素数．由于对于 $e > 2$，模 $p^2$（或 $2p^2$）的原根也是模 $p^e$（或 $2p^e$）的原根，所以，最小原根的上界 $O\left(p^{0.25+\epsilon}\right)$ 对于所有情形都成立．

Fridlander[5]和 Salié[6]证明了素数 $p$ 的最小原根 $g_p = \Omega(\log p)$．

这保证了暴力找一个数的最小原根时，复杂度可以接受．

## Carmichael 函数

相对于模 $m$ 元素的阶这一局部概念，Carmichael 函数是一个全局概念．它是所有与 $m$ 互素的整数的幂次的最小公共循环节．

**Carmichael 函数**

$m \in \mathbf{N}_+$ $\lambda(m)$ $a^n \equiv 1 \pmod{m}$ $a \perp m$
$n$ $\lambda : \mathbf{N}_+ \to \mathbf{N}_+$ **Carmichael 函数**

根据性质 2，能够使得 $a^n \equiv 1 \pmod{m}$ 对于所有 $a \perp m$ 都成立，意味着 $\delta_m(a) \mid n$ 对于所有 $a \perp m$ 都成立．也就是说，符合这一条件的正整数 $n$，一定是全体 $\delta_m(a)$ 的公倍数．因此，最小的这样的 $n$ 就是它们的最小公倍数：

$$\lambda(m) = \operatorname{lcm}\{\delta_m(a) : a \perp m\}.$$

这也常用作 Carmichael 函数的等价定义．

反复应用性质 5 可知，一定存在某个元素 $a \perp m$ 使得 $\delta_m(a) = \lambda(m)$．因此，上式也可以写作

$$\lambda(m) = \max\{\delta_m(a) : a \perp m\}.$$

取得这一最值的元素 $a \perp m$ 也称为模 $m$ 的 **$\lambda$-原根**．它对于所有模数 $m$ 都存在．

### 递推公式

Carmichael 函数是一个 数论函数．本节讨论它的一个递推公式，并由此给出原根存在定理的另一个证明．

虽然不是积性函数，但是计算 Carmichael 函数时，同样可以对互素的因子分别处理．

**引理**

$m_1, m_2$ $\lambda(m_1 m_2) = [\lambda(m_1), \lambda(m_2)]$

**证明**

$a_1$ $a_2$ $m_1$ $m_2$ $\lambda$ $m = m_1 m_2$ $a \perp m$ $a \equiv a_i \pmod{m_i}$ $i = 1, 2$ $a^{\lambda(m)} \equiv 1 \pmod{m}$ $i = 1, 2$ $a_i^{\lambda(m)} \equiv 1 \pmod{m_i}$ $a_i$ $\lambda(m_i) = \delta_{m_i}(a_i) \mid \lambda(m)$ $[\lambda(m_1), \lambda(m_2)] \mid \lambda(m)$

$a \perp m$ $i = 1, 2$ $a^{[\lambda(m_1), \lambda(m_2)]} \equiv 1 \pmod{m_i}$ $a^{[\lambda(m_1), \lambda(m_2)]} \equiv 1 \pmod{m}$ $a \perp m$ $\lambda(m) \mid [\lambda(m_1), \lambda(m_2)]$

因此，接下来只要计算 Carmichael 函数在素数幂处的取值．首先，处理 2 的幂次的情形．

**引理**

$m = 2^e$ $e \in \mathbf{N}_+$ $\lambda(2) = 1$ $\lambda(4) = 2$ $e \geq 3$ $\lambda(m) = 2^{e-2}$

**证明**

$m = 2, 4$ $m = 2^e$ $e \geq 3$ $\lambda(m) \leq 2^{e-2}$ $2^{e-2}$

$$5^{2^{e-3}} = (1 + 2^2)^{2^{e-3}} = 1 + 2^2 \times 2^{e-3} = 1 + 2^{e-1} \not\equiv 1 \pmod{2^e}.$$

$\delta_m(5)$ $2^{e-3}$ $\delta_m(5) \mid 2^{e-2}$ $5$ $2^{e-2}$ $\lambda(m) = 2^{e-2}$

然后，处理奇素数幂的情形．

**引理**

$m = p^e$ $p$ $e \in \mathbf{N}_+$ $\lambda(m) = p^{e-1}(p - 1)$

**证明**

$e=1$ $m=p$

$p$ $a$ $x^{\lambda(p)}\equiv 1 \pmod{p}$ $p$

$p-1$ $p-1\le\lambda(p)$

$\lambda(p)\mid\varphi(p)=p-1$ $\lambda(p)=p-1$

$m=p^e$ $e>1$ $1+p$ $p^{e-1}$

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

$\delta_m(1+p)=p^{e-1}$ $p$ $g$ $g^{\delta_m(g)}\equiv 1 \pmod{p}$

$p-1\mid\delta_m(p)$

$$p^{e-1}(p-1)=[\delta_m(p),p^{e-1}]\mid\lambda(m)\mid\varphi(m)=p^{e-1}(p-1).$$

$\lambda(m)=p^{e-1}(p-1)$

将本节的结果简单归纳，就得到 Carmichael 函数的递推公式：

**定理**

$m$

$$\lambda(m)=\begin{cases}\varphi(m), & \text{if } m=1,2,4,p^e \text{ for odd prime } p \text{ and } e\ge 1,\\ \frac{1}{2}\varphi(m), & \text{if } m=2^e,\ e\ge 3,\\ \operatorname{lcm}\{\lambda(p_1^{e_1}),\lambda(p_2^{e_2}),\cdots,\lambda(p_s^{e_s})\}, & \text{if } m=p_1^{e_1}p_2^{e_2}\cdots p_s^{e_s} \text{ for distinct } p_1,p_2,\cdots,p_s.\end{cases}$$

利用该递推公式可以加强前文的结果：

**推论**

$m_1,m_2$ $\lambda([m_1,m_2])=[\lambda(m_1),\lambda(m_2)]$

比较原根和 Carmichael 函数的定义可知，模 $m$ 的原根存在，当且仅当 $\lambda(m)=\varphi(m)$．从 Carmichael 函数的递推公式中，容易归纳出如下结果：

**推论**

$m$ $m=1,2,4,p^e,2p^e$ $p$ $e\in\mathbf{N}_+$

由于本节对于递推公式的证明并没有用到原根存在定理，因此，这就构成了对该定理的又一个证明．

## Carmichael 数

利用 Carmichael 函数，可以讨论 Carmichael 数（卡迈克尔数，OEIS:A002997）的性质与分布．这是 Fermat 素性测试 一定无法正确排除的合数．

**Carmichael 数**

$n$ $a \perp n$ $a^{n-1} \equiv 1 \pmod{n}$ $n$

**Carmichael 数**

最小的 Carmichael 数是 $561 = 3 \times 11 \times 17$．

由 Carmichael 函数的定义可知，合数 $n$ 是 Carmichael 数当且仅当 $\lambda(n) \mid n-1$，其中 $\lambda(n)$ 为 Carmichael 函数．进一步地，可以得到如下判断合数 $n$ 是否为 Carmichael 数的方法：

**Korselt 判别法**[7]

$n$ $n$ $n$ $p$ $(p-1) \mid (n-1)$

**证明**

$\lambda(n) \mid (n-1)$ $n$

$p$ $p \mid \lambda(n)$ $p \nmid (n-1)$

$(p-1) \mid \lambda(n)$ $(p-1) \mid (n-1)$

$n$ $p$ $n-1$ $n$

$n$

$\lambda(n) = \operatorname{lcm}\{p-1 : p \mid n\}$ $(p-1) \mid (n-1)$ $p$

$\lambda(n) \mid (n-1)$

从这一判别法出发，可以建立 Carmichael 数的一些简单性质：

**推论**

$3$

**证明**

$p_1, p_2$ $n = p_1 p_2$ $n = p_1 p_2$

$(p_i - 1) \mid (n - 1)$

$$n - 1 = p_1 p_2 - 1 \equiv p_2 - 1 \pmod{p_1 - 1}.$$

$(p_1 - 1) \mid (p_2 - 1)$ $(p_2 - 1) \mid (p_1 - 1)$ $p_1 = p_2$

$n$ $3$

利用解析数论还可以得到 Carmichael 数分布的一些性质．设 $C(n)$ 为小于等于 $n$ 的 Carmichael 数个数．Alford, Granville, and Pomerance[8]证明，对于充分大的 $n$，有 $C(n) > n^{2/7}$．由此，Carmichael 数有无限多个．在这之前，Erdős[9]已经证明，$C(n) < n \exp\left(-c\frac{\ln n \ln\ln\ln n}{\ln\ln n}\right)$，其中 $c$ 为常数．因此，Carmichael 数的分布（相对于素数来说）十分稀疏．实际上，有[10] $C(10^9) = 646$，$C(10^{18}) = 1\,401\,644$．

## 参考资料与注释

- Primitive root modulo n - Wikipedia
- The order of a unit - Course Notes
- The primitive root theorem - Amin Witno's notes
- Carmichael function - Wikipedia
- Carmichael's Lambda Function - Brilliant Math & Science Wiki
- Carmichael number - Wikipedia
- Carmichael Number - Wolfram MathWorld

---

*Sci. Sinica* ↵

↵

↵

↵

↵

↵

↵

↵

↵

$10^{20}$ ↵

---