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

定义（指数与原根）

设m是大于1的整数，a与m互素. 使得$a^e \equiv 1 \bmod m$的最小正整数e被称为a对模m的**指数(或阶)**，记作$\mathrm{ord}_m(a)$. 如果$\mathrm{ord}_m(a) = \varphi(m)$，则称$a$为模$m$的**原根**. 并不是对于任意大于1的整数$m$都有模$m$的原根.

定理

设m是大于1的整数，a与m互素.

1. 整数d使得$a^d \equiv 1 \bmod m$当且仅当$\mathrm{ord}_m(a) \mid d$.
2. 如果$n \mid m$，则$\mathrm{ord}_n(a) \mid \mathrm{ord}_m(a)$.
3. 如果$ab \equiv 1 \bmod m$，则$\mathrm{ord}_m(a) = \mathrm{ord}_m(b)$.
4. 如果a是模m的原根，则$\{a^0, a^1, a^2, \ldots, a^{\varphi(m)-1}\}$构成模$m$的一个简化剩余系.
5. $a^k \equiv a^l \bmod m$当且仅当$k \equiv l \bmod \mathrm{ord}_m(a)$
6. $\mathrm{ord}_m(a^k) = \dfrac{\mathrm{ord}_m(a)}{(\mathrm{ord}_m(a), k)}$，其中$k$是非负整数.
7. 如果模m有原根，则模m的原根的个数为$\varphi(\varphi(m))$.

定理

设m是大于1的整数，a,b均与m互素.

1. 存在$c=a^sb^t$使得$\mathrm{ord}_m(c)=[\mathrm{ord}_m(a),\mathrm{ord}_m(b)]$，其中$s=\frac{\mathrm{ord}_m(a)}{u}$, $t=\frac{\mathrm{ord}_m(b)}{v}$，而$u,v$是使得
$$u\mid \mathrm{ord}_m(a), v\mid \mathrm{ord}_m(b), uv=[\mathrm{ord}_m(a),\mathrm{ord}_m(b)], (u,v)=1.$$
都成立的一对整数.
2. 如果$(\mathrm{ord}_m(a),\mathrm{ord}_m(b))=1$，则$\mathrm{ord}_m(ab)=\mathrm{ord}_m(a)\cdot\mathrm{ord}_m(b)$.
3. 一般地，存在整数g使得$\mathrm{ord}_m(g)=[\mathrm{ord}_m(a_1),\mathrm{ord}_m(a_2),\ldots,\mathrm{ord}_m(a_k)]$，其中$2\le k\le\varphi(m)$.

定理

设m是大于1的整数, a, b均与m互素.

1. 存在$c = a^s b^t$使得$\mathrm{ord}_m(c) = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)]$, 其中$s = \frac{\mathrm{ord}_m(a)}{u}$, $t = \frac{\mathrm{ord}_m(b)}{v}$, 而$u, v$是使得
$$u \mid \mathrm{ord}_m(a), v \mid \mathrm{ord}_m(b), uv = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)], (u, v) = 1.$$
都成立的一对整数.
2. 如果$(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$, 则$\mathrm{ord}_m(ab) = \mathrm{ord}_m(a) \cdot \mathrm{ord}_m(b)$.
3. 一般地, 存在整数g使得$\mathrm{ord}_m(g) = [\mathrm{ord}_m(a_1), \mathrm{ord}_m(a_2), \ldots, \mathrm{ord}_m(a_k)]$, 其中$2 \leq k \leq \varphi(m)$.

定理

设m, n互素. $(a_1, m) = (a_2, n) = 1$.

1. 存在整数a使得$(a, mn) = 1$且$\mathrm{ord}_{mn}(a) = [\mathrm{ord}_m(a_1), \mathrm{ord}_m(a_2)]$, 且$a$可以通过中国剩余定理计算得到.
2. 如果$a_1 = a_2$, 则$\mathrm{ord}_{mn}(a_1) = [\mathrm{ord}_m(a_1), \mathrm{ord}_n(a_1)]$.

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

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

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$g^{p-1} \equiv 1 \bmod p$，从而有$\delta \le p-1$.
另一方面，由于δ是$\mathrm{ord}_p(1), \mathrm{ord}_p(2), \ldots, \mathrm{ord}_p(p-1)$的公倍数，所以

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

这表明

$$1^\delta \equiv 1 \bmod p, 2^\delta \equiv 1 \bmod p, \ldots, (p-1)^\delta \equiv 1 \bmod p.$$

也是就是说，同余方程

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

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

定理

设p是奇素数, $q_1, q_2, \ldots, q_s$是$p-1$的所有不同的素因数. g是模p原根当且仅当

$$g^{\frac{p-1}{q_i}} \not\equiv 1(\bmod p), \quad i = 1, 2, \ldots, s.$$

"必要性"是显然的.

"充分性:" 反证法. 假设模p的指数$e = \mathrm{ord}_p(g) < p-1$. 那么$e \mid (p-1)$, 且$\frac{p-1}{e} > 1$. 因此存在一个素数$q$使得$q \mid \frac{p-1}{e}$, 即存在整数$u$使得

$$\frac{p-1}{e} = u \cdot q \quad 或 \quad \frac{p-1}{q} = u \cdot e.$$

于是, 我们有

$$g^{\frac{p-1}{q}} = (g^e)^u \equiv 1 \bmod p.$$

这与已知条件矛盾.

示例: 求模$p = 23$的原根.

这里$p - 1 = 22 = 2 \cdot 11$, $p - 1$的真因子有$q_1 = 2, q_2 = 11$.
要验证a是否为模m的原根, 需要保证$(a, p) = 1$, 并验证

$$a^{\frac{p-1}{q_1}} \equiv a^{11} \not\equiv 1 \bmod p, \quad a^{\frac{p-1}{q_2}} \equiv a^2 \not\equiv 1 \bmod p$$

是否成立.

先求$a = 2$对模23的指数:

$$2^2 \equiv 4 \bmod 23$$

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

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

再求$a = 3$对模23的指数:
$$3^2 \equiv 9 \bmod 23$$
$$3^3 \equiv 4 \bmod 23$$
$$3^{11} = (3^3)^3 \cdot 3^2 \equiv 4^3 \cdot 9 \equiv (-5) \cdot 9 \equiv 1 \bmod 23$$
所以$\mathrm{ord}_{23}(3) = 11$, 3不是模23的原根;

再求$a = 4$对模23的指数:
$$4^2 \equiv -7 \bmod 23$$
$$4^{11} = (4^4)^2 \cdot 4^3 \equiv 3^2 \cdot (-5) \equiv 1 \bmod 23$$
所以$\mathrm{ord}_{23}(4) = 11$, 4不是模23的原根;

再求$a = 5$对模23的指数:
$$5^2 \equiv 9 \bmod 23$$
$$5^{11} = (5^4)^2 \cdot 5^3 \equiv 4^2 \cdot 10 \equiv 4 \cdot (-6) \equiv -1 \bmod 23$$
$$5^{22} \equiv 1 \bmod 23$$
所以$\mathrm{ord}_{23}(5) = 22$, 5是模23的原根.

3. 原根存在的充要条件

先考虑模m有原根的必要条件.

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

推论

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

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

令

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

即β是$\varphi(2^{\alpha_1}),\varphi(p_2^{\alpha_2}),\varphi(p_3^{\alpha_3}),\ldots,\varphi(p_s^{\alpha_s})$的最小公倍数.
由于$\mathrm{ord}_{p^\alpha}(a)|\varphi(p^\alpha)$，从而$\beta$是$\mathrm{ord}_{2^{\alpha_1}}(a),\mathrm{ord}_{p_2^{\alpha_2}}(a),\ldots,\mathrm{ord}_{p_s^{\alpha_s}}(a)$的公倍数，所以

$$[\mathrm{ord}_{2^{\alpha_1}}(a),\mathrm{ord}_{p_2^{\alpha_2}}(a),\ldots,\mathrm{ord}_{p_s^{\alpha_s}}(a)]\mid\beta$$

即

$$\mathrm{ord}_m(\alpha)\mid\beta.$$

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

所以,

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

接着于是有

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

使用数学归纳法可以证明这个等式，如果a是奇数，则$a^{2^{l-2}} \equiv 1 \bmod 2^l (l \geq 3)$成立.
设$l = n$时成立，即$a^{2^{n-2}} \equiv 1 \bmod 2^n$，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$a^{2^{n-1}} - 1 \equiv 0 \bmod 2^{n+1}$，即$a^{2^{n-1}} \equiv 1 \bmod 2^{n+1}$.
这个结论说明，$\mathrm{ord}_{2^l}(a) \mid 2^{l-2} (l \geq 3)$.
所以，当$\alpha_1 \geq 3$时，我们有:

$$\mathrm{ord}_m(a) \mid [2^{\alpha_1 - 2}, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})].$$

于是,

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

重新记右边的最小公倍数为β, 即

$$\text{当}m = p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_s^{\alpha_s}\text{时}, \text{令}\beta = [1, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})].$$

$$\text{当}m = 2p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_s^{\alpha_s}\text{时}, \text{令}\beta = [1, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})].$$

$$\text{当}m = 4p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_s^{\alpha_s}\text{时}, \text{令}\beta = [2, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})].$$

$$\text{当}m = 2^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_s^{\alpha_s}\text{时}, \text{令}\beta = [2^{\alpha_1-2}, \varphi(p_2^{\alpha_2}), \varphi(p_3^{\alpha_3}), \ldots, \varphi(p_s^{\alpha_s})].$$

定理

模m存在原根仅当$m=1$，或2，或4，或p^α,或$2p^\alpha$，其中p是奇素数.

证明：假设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$m=2^\alpha p_1^{\alpha_1}\ldots p_s^{\alpha_s}(\alpha\geq 2, s\geq 1)$，或是$m=2^\alpha p_1^{\alpha_1}\ldots p_s^{\alpha_s}(\alpha\geq 0, s\geq 2)$.
$<1>$，如果$m=2^\alpha(\alpha\geq 3)$，则$\mathrm{ord}_{2^\alpha}(a)\,|\,2^{\alpha-2}$，于是$\mathrm{ord}_m(a)<2^{\alpha-1}=\varphi(m)$，所以这时模$m$没有原根；
$<2>$，如果$m=2^\alpha p_1^{\alpha_1}\ldots p_s^{\alpha_s}(\alpha\geq 2, s\geq 1)$，即$m=4p_1^{\alpha_1}\ldots p_s^{\alpha_s}(s\geq 1)$或$m=2^\alpha p_1^{\alpha_1}\ldots p_s^{\alpha_s}(\alpha\geq 3, s\geq 1)$.

- 对应前述的$\beta=[2,\varphi(p_1^{\alpha_1}),\varphi(p_2^{\alpha_2}),\ldots,\varphi(p_s^{\alpha_s})]$，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．于是，

$$\begin{aligned}\beta &= [2,\varphi(p_1^{\alpha_1}),\varphi(p_2^{\alpha_2}),\ldots,\varphi(p_s^{\alpha_s})]=[\varphi(p_1^{\alpha_1}),\varphi(p_2^{\alpha_2}),\ldots,\varphi(p_s^{\alpha_s})]\\ &\leq \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\varphi(p_s^{\alpha_s})<2\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\varphi(p_s^{\alpha_s})=\varphi(m).\end{aligned}$$

  所以，对于任意的a满足$(a,m)=1$，都有$\mathrm{ord}_m(a)<\varphi(m)$，这时模$m$没有原根；

- 类似地，$\beta=[2^{\alpha-2},\varphi(p_1^{\alpha_1}),\varphi(p_2^{\alpha_2}),\ldots,\varphi(p_s^{\alpha_s})]\leq$
  $2^{\alpha-2}\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\varphi(p_s^{\alpha_s})<2^{\alpha-1}\varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\ldots\varphi(p_s^{\alpha_s})=\varphi(m)$.
  所以，对于任意的a满足$(a,m)=1$，都有$\mathrm{ord}_m(a)<\varphi(m)$，这时模$m$没有原根.

$<3>$, 如果$m=2^{\alpha}p_1^{\alpha_1}\dots p_s^{\alpha_s}(\alpha\geq 0, s\geq 2)$, 即$m=p_1^{\alpha_1}\dots p_s^{\alpha_s}(s\geq 2)$
或$m=2p_1^{\alpha_1}\dots p_s^{\alpha_s}(s\geq 2)$ 或$m=4p_1^{\alpha_1}\dots p_s^{\alpha_s}(\alpha\geq 3,\geq 2)$. 对应地, 我们有
$\varphi(m)=\varphi(p_1^{\alpha_1})\dots\varphi(p_s^{\alpha_s})$.
$\varphi(m)=\varphi(2)\varphi(p_1^{\alpha_1})\dots\varphi(p_s^{\alpha_s})=\varphi(p_1^{\alpha_1})\dots\varphi(p_s^{\alpha_s})$.
$\varphi(m)=\varphi(4)\varphi(p_1^{\alpha_1})\dots\varphi(p_s^{\alpha_s})=2\varphi(p_1^{\alpha_1})\dots\varphi(p_s^{\alpha_s})$.
$\varphi(m)=\varphi(2^{\alpha})\varphi(p_1^{\alpha_1})\dots\varphi(p_s^{\alpha_s})=2^{\alpha-1}\varphi(p_1^{\alpha_1})\dots\varphi(p_s^{\alpha_s})$.

对应前述的$\mathrm{ord}_m(a)\,|\,\beta$, 我们得到
$\beta=[1,\varphi(p_1^{\alpha_1}),\dots,\varphi(p_s^{\alpha_s})]<\varphi(p_1^{\alpha_1})\dots\varphi(p_s^{\alpha_s})=\varphi(m)$.
$\beta=[1,\varphi(p_1^{\alpha_1}),\dots,\varphi(p_s^{\alpha_s})]<\varphi(p_1^{\alpha_1})\dots\varphi(p_s^{\alpha_s})=\varphi(m)$.
$\beta=[2,\varphi(p_1^{\alpha_1}),\dots,\varphi(p_s^{\alpha_s})]<\varphi(p_1^{\alpha_1})\dots\varphi(p_s^{\alpha_s})<2\varphi(p_1^{\alpha_1})\dots\varphi(p_s^{\alpha_s})=\varphi(m)$.
$\beta=[2^{\alpha-2},\varphi(p_1^{\alpha_1}),\dots,\varphi(p_s^{\alpha_s})]<2^{\alpha-1}\varphi(p_1^{\alpha_1})\dots\varphi(p_s^{\alpha_s})=\varphi(m)$.
所以, 对于任意的a满足$(a,m)=1$, 都有$\mathrm{ord}_m(a)<\varphi(m)$, 这时模$m$没有原根.

如果模m有原根的话, 只能是1, 或2, 或4, 或p^{α}, 或是$2p^{\alpha}$.

定理

如果g是模$p^{\alpha+1}$的原根, 则g必是模p^α的原根, 其中p为奇素数, $\alpha \geq 1$.

证明: 设$\mathrm{ord}_{p^\alpha}(g) = \delta$, 从而$\delta \mid \varphi(p^\alpha)$. 同时, $g^\delta \equiv 1 \bmod p^\alpha$, 即存在整数$k$使得$g^\alpha = kp^\alpha + 1$. 于是我们有

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

其中A为整数. 这表明

$$(g^\delta)^p \equiv g^{p\delta} \equiv 1 \bmod p^{\alpha+1}.$$

从而有$\mathrm{ord}_{p^{\alpha+1}}(g) \mid p\delta$, 即$\varphi(p^{\alpha+1}) \mid p\delta$, 也即$p^{\alpha-1}(p-1) \mid \delta$.
而$\varphi(p^\alpha) = p^{\alpha-1}(p-1)$, 所以$\varphi(p^\alpha) \mid \delta$. 因此, $\delta = \varphi(p^\alpha)$, g也是模p^α的原根. $\diamond$

定理

设g是模p^α的原根，则$\mathrm{ord}_{p^{\alpha+1}}(g)=\varphi(p^\alpha)$，或者$\mathrm{ord}_{p^{\alpha+1}}(g)=\varphi(p^{\alpha+1})$，其中$p$为奇素数，$\alpha\geq 1$.

证明：由于$p^\alpha \mid p^{\alpha+1}$，由指数的性质可知

$$\mathrm{ord}_{p^\alpha}(g) \mid \mathrm{ord}_{p^{\alpha+1}}(g)$$

所以有$\varphi(p^\alpha) \mid \mathrm{ord}_{p^{\alpha+1}}(g)$，即存在整数$k$使得$\mathrm{ord}_{p^{\alpha+1}}(g)=k\cdot\varphi(p^\alpha)$.
另一方面，$\mathrm{ord}_{p^{\alpha+1}} \mid \varphi(p^{\alpha+1})$，存在整数$k'$使得$\varphi(p^{\alpha+1})=k'\cdot\mathrm{ord}_{p^{\alpha+1}}(g)$，从而有

$$\varphi(p^{\alpha+1})=k'\cdot k\cdot\varphi(p^\alpha),$$

也即$p^\alpha(p-1)=kk'p^{\alpha-1}(p-1)$.
于是，我们有$kk'=p$. 这表明$k=1$且$k'=p$，或者是$k=p$且$k'=1$.

$k=1$且$k'=p$，有$\mathrm{ord}_{p^{\alpha+1}}(g)=\varphi(p^\alpha)$;
$k=p$且$k'=1$，有$\mathrm{ord}_{p^{\alpha+1}}(g)=p\varphi(p^\alpha)=p\cdot p^{\alpha-1}(p-1)=p^\alpha(p-1)=\varphi(p^{\alpha+1})$. ◇

定理

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

证明：首先证明对这个原根g和任意的$\alpha\geq 1$总有

$$g^{\varphi(p^\alpha)}=1+r_\alpha p^\alpha$$

成立，其中r_α是一个整数，使得$p\nmid r_\alpha$.
归纳法：$\alpha=1$时就是已知条件. 假设$\alpha=n$时，有$g^{\varphi(p^n)}=1+r_n p^n$且$p\nmid r_n$.
当$\alpha=n+1$时，由于$\varphi(p^{k+1})=p\varphi(p^k)$，所以：

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

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

这样, 对于满足定理要求的g来说有

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

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

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

这个过程继续下去可知, 对于任意的$\alpha \geq 1$和满足定理要求的g是模p^α的原根. $\diamond$

定理

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

因为$g \equiv g' \bmod p$. 所以，对于任意的$i \geq 1$有$g^i \equiv (g')^i \bmod p$.
而g'是模p的原根，对于$1 \leq i < p-1$，都有

$$(g')^i \not\equiv 1 \bmod p.$$

从而，对于$1 \leq i < p-1$，都有

$$g^i \not\equiv 1 \bmod p.$$

即g也是模p的原根. $\diamond$

另外还可以证明，在这p个g中，除了一个外，其他的g都满足

$$g^{p-1} = 1 + rp$$

其中r是一个整数，使得$p \nmid r$.

注意到
$$g^{p-1}=(g'+tp)^{p-1}=g'^{p-1}+(p-1)g'^{p-2}(tp)+Ap^2$$
其中$t=0,1,\ldots,p-1$, A是一个整数.
由于g'是模p的原根, 可设$(g')^{p-1}=1+ap$, 从而有

$$g^{p-1}=1+\Big((p-1)(g')^{p-2}t+a\Big)p+Ap^2=1+\Big((p-1)(g')^{p-2}t+(a+Ap)\Big)p.$$

又由于$(p,p-1)=1$且$(p,g')=1$, 因此$(p,(p-1)(g')^{p-2})=1$.
所以关于t的一次同余方程$(p-1)(g')^{p-2}t+(a+Ap)\equiv 0 \bmod p$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.

设p是奇素数, g'为模p的原根, 则

$$g=g', g=g'+p, g=g'+2p, \ldots, g=g'+(p-1)p$$

都是模p的原根, 且它们当中只有一个不满足条件$g^{p-1}=1+rp, p\nmid r$, 其余都满足.

在上述结论中, 如果我们还要求g'为奇数. 如果原根g'不是奇数(即是偶数), 则令$g'' := g' + p$, 那么g''是一个为奇数的模p的原根, 可以用g''来构造g.

由于$t = 0, 1, 2, \ldots, p-1$中至少有2个偶数, 从而$g = g' + tp(t = 0, 1, \ldots, p-1)$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$g$满足

- 是奇数;
- 是模p的原根;
- 满足$g^{p-1} = 1 + rp$且$p \nmid r$.

综上, 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

$$(\tilde{g})^{p-1} = 1 + rp$$

其中r是一个整数, 使得$p \nmid r$.

找到的这个$\tilde{g}$, 即找到了模p^{α}的一个原根.

由于$\tilde{g}$是奇数, 那么对于任意整数d,

$$\tilde{g}^d \equiv 1 \bmod p^\alpha$$

当且仅当

$$\tilde{g}^d \equiv 1 \bmod 2p^\alpha.$$

一方面, 如果$\tilde{g}^d \equiv 1 \bmod 2p^\alpha$, 则显然有$\tilde{g}^d \equiv 1 \bmod p^\alpha$.
另一方面, 如果$\tilde{g}^d \equiv 1 \bmod p^\alpha$, 则$p^\alpha \mid \tilde{g}^d - 1$,. 而$2 \mid \tilde{g}^d - 1$, 且$(2, p) = 1$,
所以$[2, p^\alpha] = 2p^\alpha$, 且$2p^\alpha \mid \tilde{g}^d - 1$, 即$\tilde{g}^d \equiv 1 \bmod 2p^\alpha$.

这样, 我们有

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

即找到的这个$\tilde{g}$也是模$2p^\alpha$的原根.

整理上述的几个结论:

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', 可以构造一个为奇数的模p的原根$\tilde{g}$满足

$$(\tilde{g})^{p-1} = 1 + rp$$

   其中r是一个整数, 使得$p \nmid r$;
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,已知模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$2p^\alpha$，其中p为奇素数，$\alpha\geq 1$.

在指数的性质中，已经证明了模m有原根的必要条件就是$m=1$,或2,或4,或p^α,或$2p^\alpha$.

所以,下面需要证明模m有原根的充分条件也是$m=1$,或2,或4,或p^α,或$2p^\alpha$

事实上，容易检查:

- 如果$m=1$，模1的原根就是1：$\varphi(m)=1, 1^1=1$;
- 如果$m=2$，模2的原根就是1：$\varphi(m)=1, 1^1=1$;
- 如果$m=4$，模4的原根就是3：$\varphi(m)=2, 3^1=3, 3^2=9\equiv 1 \bmod 4$;
- 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.

3. 指标

我们知道，当g是模m的原根时，$g^1, g^2, \ldots, g^{\varphi(m)-1}, g^{\varphi(m)}$两两模$m$不同余. 它们构成了一个模$m$的简化剩余系. 换句话说，$g$是模$m$的一个原根，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，在$1 \sim \varphi(m)$之间存在唯一的整数$r$，使得

$$g^r \equiv a \bmod m.$$

把这个整数r称为以g为底的a对模m的指标，记作$\mathrm{ind}_g a$，或$\mathrm{ind} a$.
特别地，在密码学中，$\mathrm{ind}_g a$通常被称为以g为底的a对模m的'离散对数'，记作$\log_g a$.

例如，$g = 5$是模$m = 17$的一个原根，且

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

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...

重要的是，当m非常大时，给定模m的原根g和一个模m的简化剩余a，计算指标$\mathrm{ind}_g a$，或者说计算离散对数$\log_g a$一般是非常困难的计算数学问题.

定理

设m是大于1的整数，g是模m原根. 如果$g^s \equiv a \bmod m$，则$s \equiv \mathrm{ind}_g a \bmod \varphi(m)$.

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$\mathrm{ind}_6 9 = 30$，求同余方程$x^5 \equiv 9 \bmod 41$的解：

设x_1是这个方程的解. 因为$(9, 41) = 1$，所以$(x_1^5, 41) = 1$，从而$(x_1, 41) = 1$.
因为6是模41的原根，所以可设$x_1 = 6^{y_1} \bmod 41$，则$x_1^5 \equiv 9 \bmod 41$就等价于

$$6^{5y_1} \equiv 9 \bmod 41.$$

于是，我们有

$$5y_1 \equiv \mathrm{ind}_6 9 \bmod 40,$$

即

$$5y_1 \equiv 30 \bmod 40$$

求解可得，$y_1 \equiv 6, 14, 22, 30, 38 \bmod 40$. 对应原同余方程的解有

$$x \equiv 6^6 \bmod 41, x \equiv 6^{14} \bmod 41, \ldots\ldots$$

定理

设m是大于1的整数, g是模m原根. $a_1, \ldots, a_n$均与m互素, 则

$$\mathrm{ind}_g(a_1 \ldots a_n) \equiv \mathrm{ind}_g a_1 + \ldots + \mathrm{ind}_g a_n \bmod \varphi(m).$$

事实上,

$$\left.\begin{array}{r} g^{\mathrm{ind}_g(a_1)} \equiv a_1 \bmod m \\ g^{\mathrm{ind}_g(a_2)} \equiv a_2 \bmod m \\ \ldots\ldots \\ g^{\mathrm{ind}_g(a_n)} \equiv a_n \bmod m \end{array}\right\} \Longrightarrow (a_1 a_2 \ldots a_n) \equiv g^{\mathrm{ind}_g(a_1)} g^{\mathrm{ind}_g(a_2)} \ldots g^{\mathrm{ind}_g(a_n)} \bmod m$$

$$\Longrightarrow (a_1 a_2 \ldots a_n) \equiv g^{\mathrm{ind}_g(a_1)+\mathrm{ind}_g(a_2)+\ldots+\mathrm{ind}_g(a_n)} \bmod m$$

$$\Longrightarrow \mathrm{ind}_g(a_1) + \mathrm{ind}_g(a_2) + \ldots + \mathrm{ind}_g(a_n) \equiv \mathrm{ind}_g(a_1 a_2 \ldots a_n) \bmod \varphi(m) \qquad \diamond$$

指数与指标间的联系:

设g为模m的原根, a与m互素. a的指数记作$\mathrm{ord}_m(a)$, 其指标记为$\mathrm{ind}_g a$, .
我们知道$g^{\mathrm{ind}_g a} \equiv a \bmod m$,

$$\begin{aligned}\mathrm{ord}_m(a) &= \mathrm{ord}_m(g^{\mathrm{ind}_g a}) \\ &= \frac{\mathrm{ord}_m(g)}{(\mathrm{ord}_m(g), \mathrm{ind}_g a)} \\ &= \frac{\varphi(m)}{(\varphi(m), \mathrm{ind}_g a)}\end{aligned}$$

即

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

由此可见,

定理

设m是大于1的整数, g是模m原根. 如果a是模m的原根, 当且仅当$(\varphi(m), \mathrm{ind}_g a) = 1$.

定理

设g是模m原根. 在模m的简化剩余系中, 指数为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

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

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

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

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

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

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

定理

设g是模m的一个原根，a与m互素，则同余方程$x^n \equiv a \bmod m$有解当且仅当$(n, \varphi(m)) \mid \mathrm{ind}_g a$. 如果有解，解数为$(n, \varphi(m))$.

证明: "必要性:" 设同余式有解$x \equiv x_0 \bmod m$，即$x_0^n \equiv a \bmod m$. 因为$(a, m) = 1$，所以$(x_0^n, m) = 1$，从而$(x_0, m) = 1$. 于是，存在一个整数u使得$x_0 \equiv g^u \bmod m$，从而使得$g^{nu} \equiv a \bmod m$. 所以我们有

$$nu \equiv \mathrm{ind}_g a \bmod \varphi(m).$$

这表明，一次同余式$ny \equiv \mathrm{ind}_g a \bmod \varphi(m)$有解，从而必有$(n, \varphi(m)) \mid \mathrm{ind}_g a$.

"充分性:" 如果$(n, \varphi(m)) \mid \mathrm{ind}_g a$，则一次同余式$ny \equiv \mathrm{ind}_g a \bmod \varphi(m)$有解，且解数为$(n, \varphi(m))$. 不妨设$y \equiv u \bmod \varphi(m)$是一个解，则$nu \equiv \mathrm{ind}_g a \bmod \varphi(m)$，即存在整数$k$使得$nu = k\varphi(m) + \mathrm{ind}_g a$，从而有

$$g^{nu} = g^{k\varphi(m)+\mathrm{ind}_g a} = g^{k\varphi(m)} g^{\mathrm{ind}_g a} \equiv a \bmod m,$$

即$x \equiv y^u \bmod m$就是原n次同余方程的一个解. $\diamond$

推论

设g是模m的一个原根，a与m互素，则同余方程$x^n \equiv a \bmod m$有解当且仅当

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

其中$d = (n, \varphi(m))$.

证明：我们已经知道，同余方程$x^n \equiv a \bmod m$有解当且仅当一次同余式

$$ny \equiv \mathrm{ind}_g a \bmod \varphi(m)$$

有解．而这等价于$n, \varphi(m) \mid \mathrm{ind}_g a$，即$\mathrm{ind}_g a \equiv 0 \bmod \varphi(m)$．两端同乘以$\frac{\varphi(m)}{d}$，同余式仍然成立，从而我们得到

$$\frac{\varphi(m)}{d} \mathrm{ind}_g a \equiv 0 \bmod \varphi(m).$$

即存在整数k使得所以$\frac{\varphi(m)}{d} \mathrm{ind}_g a = k \cdot \varphi(m)$，所以，

$$a^{\frac{\varphi(m)}{d}} \equiv (g^{\mathrm{ind}_g a})^{\frac{\varphi(m)}{d}} \equiv g^{\frac{\varphi(m)}{d} \mathrm{ind}_g a} \equiv g^{k\varphi(m)} \equiv 1 \bmod m.$$

注：使用该推论的一个好处是不需要计算$\mathrm{ind}_g a$的值.