初等数论
第五章 原根与指标

中山大学 计算机学院

1. 指数

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

$$a^e \equiv 1 \bmod m$$

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

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，$2^1 = 2, 2^2 = 4, 2^3 \equiv 1 \bmod 7$，所以2的指数为3
对$a = 3$来说，$3^1 = 3, 3^2 \equiv 2, \ldots, 3^6 \equiv 1 \bmod 7$，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: $m = 15, \varphi(m) = 8$

$1 \sim 5$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
$\mathrm{ord}_m(a)$	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".

定理

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

"必要性:"

$$\mathrm{ord}_m(a) \mid d \Longrightarrow d = k \cdot \mathrm{ord}_m(a) \Longrightarrow a^d = (a^{\mathrm{ord}_m(a)})^k \Longrightarrow a^d \equiv 1 \bmod m$$

"充分性:" 假设d使得$a^d \equiv 1 \bmod m$,
如果$\mathrm{ord}_m(a) \nmid d$, 则由欧几里德除法知，存在整数$q, r$使得

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

从而

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

而

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

从而$a^r \equiv 1 \bmod m$, 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$a^{\varphi(m)} \equiv 1 \bmod m$, 因此有$\mathrm{ord}_m(a) \mid \varphi(m)$.
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$\mathrm{ord}_{17}(5)$

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$5^{16} \equiv 1 \bmod 17$

所以$\mathrm{ord}_{17}(5) = 16$, 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$\mathrm{ord}_n(a) \mid \mathrm{ord}_m(a)$.

$$\left.\begin{array}{r} a^{\mathrm{ord}_m(a)} \equiv 1 \bmod m \\ n \mid m \end{array}\right\} \Longrightarrow a^{\mathrm{ord}_m(a)} \equiv 1 \bmod n \Longrightarrow \mathrm{ord}_n(a) \mid \mathrm{ord}_m(a)$$

定理

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

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

例如,

$$39 \equiv 5 \bmod 17 \Longrightarrow \mathrm{ord}_{17}(39) = \mathrm{ord}_{17}(5) = 16.$$

定理

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

事实上

$$(ab)^{\mathrm{ord}_m(a)} \equiv 1 \bmod m \Longrightarrow a^{\mathrm{ord}_m(a)} \cdot b^{\mathrm{ord}_m(a)} \equiv 1 \bmod m$$
$$\Longrightarrow b^{\mathrm{ord}_m(a)} \equiv 1 \bmod m \Longrightarrow \mathrm{ord}_m(b) \,|\, \mathrm{ord}_m(a).$$

类似地

$$(ab)^{\mathrm{ord}_m(b)} \equiv 1 \bmod m \Longrightarrow a^{\mathrm{ord}_m(b)} \cdot b^{\mathrm{ord}_m(b)} \equiv 1 \bmod m$$
$$\Longrightarrow a^{\mathrm{ord}_m(b)} \equiv 1 \bmod m \Longrightarrow \mathrm{ord}_m(a) \,|\, \mathrm{ord}_m(b).$$

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

例如，

$$5 \cdot 7 \equiv 1 \bmod 17 \Longrightarrow \mathrm{ord}_{17}(7) = \mathrm{ord}_{17}(5) = 16$$

定理

设m是大于1的整数, a与m互素.

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

模m两两不同余.

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

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

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

这些数正好构成了模m的一个简化剩余系.

例如, $\{5^0, 5^1, \ldots, a^{\varphi(m)-1}\}$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. $a^k \equiv a^l \bmod m$当且仅当$k \equiv l \bmod \mathrm{ord}_m(a)$.

根据欧几里德除法, 存在整数q, r和q', r'使得

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

和

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

成立, 从而有

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

以及

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

成立.

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

"充分性:" $k \equiv l \bmod \mathrm{ord}_m(a) \Longrightarrow r = r' \Longrightarrow a^k \equiv a^l \bmod m$ $\diamond$

定理

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

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

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

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

又因为$(\dfrac{\mathrm{ord}_m(a)}{d}, \dfrac{k}{d}) = 1$, 所以$\dfrac{\mathrm{ord}_m(a)}{d} \mid \mathrm{ord}_m(a^k)$.
另一方面,

$$\because (a^k)^{\frac{\mathrm{ord}_m(a)}{d}} = (a^{\mathrm{ord}_m(a)})^{\frac{k}{d}} \equiv 1 \bmod m \qquad \therefore \mathrm{ord}_m(a^k) \mid \frac{\mathrm{ord}_m(a)}{d} \qquad \diamond$$

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

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

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

证明: "充分性:" 需要说明t与rs相互整除.
先说明$t \mid (rs)$: $(ab)^{rs} = a^{rs}b^{rs} = (a^r)^s(b^s)^r \equiv 1 \bmod m \Longrightarrow t \mid (rs)$
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,

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

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

又因为r与s互素, 所以有$r \mid t$;

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

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

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

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

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

这个结论还说明,
不一定有

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

不一定有

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

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

定理

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

回忆最小公倍数的性质, 存在u, v使得

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

令

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

从而

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

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

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

一般地, 存在g使得$\mathrm{ord}_m(g) = [\mathrm{ord}_m(a_1), \mathrm{ord}_m(a_2), \ldots, \mathrm{ord}_m(a_k)]$, $2 \le k \le \varphi(m)$.
还可以看到, 如果$(\mathrm{ord}_m(a), \mathrm{ord}_m(b)) = 1$, 则有$\mathrm{ord}_m(ab) = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)]$. 如果没有该条件, 则存在$c$使得$\mathrm{ord}_m(c) = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)]$.

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

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

$$a^r \equiv 1 \bmod m \Longrightarrow a^{[r,s]} \equiv 1 \bmod m$$

$$a^s \equiv 1 \bmod n \Longrightarrow a^{[r,s]} \equiv 1 \bmod n$$

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

(要注意与"$\mathrm{ord}_m(ab) = [\mathrm{ord}_m(a), \mathrm{ord}_m(b)]$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$\mathrm{ord}_{pq}(a) = [\mathrm{ord}_p(a), \mathrm{ord}_q(a)]$. 一般地，如果$m$的标准分解式为$m = 2^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \dots p_s^{\alpha_s}$，$(a, m) = 1$，则有

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

定理

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

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

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

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

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

从而

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

可以看出，如果$a_1=a_2$，则$\mathrm{ord}_{mn}(a_1)=[\mathrm{ord}_m(a_1),\mathrm{ord}_n(a_1)]$. 如果没有条件$a_1=a_2$，则存在$a$使得$\mathrm{ord}_{mn}(a)=[\mathrm{ord}_m(a_1),\mathrm{ord}_n(a_2)]$.
与此对比，如果$(\mathrm{ord}_m(a),\mathrm{ord}_m(b))=1$，则有$\mathrm{ord}_m(ab)=[\mathrm{ord}_m(a),\mathrm{ord}_m(b)]$. 如果没有该条件，则存在$c$使得$\mathrm{ord}_m(c)=[\mathrm{ord}_m(a),\mathrm{ord}_m(b)]$.

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$\delta \leq p-1$.
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$\delta \geq p-1$. 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

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

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:

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

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

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.