§5. 原根与指数

一、原根

def 5.1 设 $(a,m)=1$，满足 $a^r\equiv 1 \pmod m$ 的最小正整数 r 叫做整数 a 模 m 的阶.

该性质是模 m 同余类的性质，即若 $a\equiv b \pmod m$，则 a 和 b 模 m 有相同的阶，于是可以谈 $\mathbb{Z}_n^*$ 中元素 $\alpha=\bar{a}=(\bar{b})$ 的阶，即满足 $\alpha^r=\bar{1}$ 的最小正整数 r.

因为模 m 的1阶元素是同余类 $\bar{1}$ 中的整数，因此 $\mathbb{Z}_m^*$ 中只有 $\bar{1}$ 是1阶元素。一般地，a 是模 m 的阶 r 满足 $1\le r\le \varphi(m)$.

Thm 5.2 设 $(a,m)=1$，r 为 a 模 m 的阶，则

1) 对每个正整数 k，$a^k\equiv 1 \pmod m$ 当且仅当 $r\mid k$，

特别地，$r\mid\varphi(m)$

2) 对每个整数 l，a^l 模 m 的阶为 $\frac{r}{(r,l)}$.

特别地，当 $(l,r)=1$ 时，a 和 a^l 模 m 有相同的阶.

证：1) 用带余除法 $k=qr+s$　$s,q\in\mathbb{Z}$ 且 $0\le s<r$

由 $a^k\equiv 1\equiv a^r \pmod m$ 和 $(a,m)=1$，可知

$$a^s=a^{k-qr}=a^k\cdot(a^r)^{-q}\equiv 1 \pmod m$$

但 r 是满足 $a^r\equiv 1 \pmod m$ 的最小正整数.

又 $0\le s<r$　故 $s=0$　从而 $k=qr$　即 k 是 r 的倍数或 $r\mid k$

反之，若 $r\mid k$，即 $k=rq$　从而 $a^k=a^{rq}=(a^r)^q\equiv 1 \pmod m$

最后：$\because a^{\varphi(m)}\equiv 1 \pmod m$　$\therefore r\mid\varphi(m)$

2) 采用群 $\mathbb{Z}_m^*$ 中的语言，记 $\alpha=\bar{a}\in\mathbb{Z}_m^*$，则对 $\forall n\in\mathbb{Z}^+$

$$(a^l)^n=1 \Leftrightarrow a^{ln}=1 \Leftrightarrow r\mid ln \Leftrightarrow \frac{r}{(r,l)}\Big|\frac{l}{(r,l)}n \Leftrightarrow \frac{r}{(r,l)}\Big| n$$

满足上式(最右边)的最小正整数 n 即是 a^l 的阶.

而满足上式(最右边)的最小正整数为 $\frac{r}{(r,l)}$

$\therefore a^l$ 的阶为 $\frac{r}{(r,l)}$.

推论5.3 设 $(a,m)=1$，则 a 模 m 的阶为 r 当且仅当以下的两条件成立：

A) $a^r \equiv 1 \pmod m$

B) 对 r 的每个素因子 p，$a^{\frac{r}{p}} \not\equiv 1 \pmod m$.

证：若 a 模 m 的阶为 r，则 $\langle A\rangle$，$\langle B\rangle$ 显然

反之，设 (A) 和 (B) 成立，设 l 是 a 模 m 的阶

由 $\langle A\rangle$ 可知：$l \mid r$ 若 $l \neq r$，则 $r=ls$，s 为大于1的整数

从而 s 有素因子 p，即 $s=pt$，$t\in\mathbb{Z}$ $\therefore r=lpt$.

而 $a^{\frac{r}{p}}=a^{lt}=(a^l)^t\equiv 1 \pmod m$

这与条件 (B) 矛盾，故 $l=r$，即 a 模 m 的阶为 r.

ex1. 对 $m=8$，$\mathbb{Z}_8^*=\{\bar{1},\bar{3},\bar{5},\bar{7}\}$，其中 $\bar{1}$ 是一阶元素，而 $\bar{3}^2=\bar{5}^2=\bar{7}^2=\bar{1}$.

故 $\bar{3},\bar{5},\bar{7}$ 均为2阶元素.

ex2. 对 $m=7$，$\mathbb{Z}_7^*=\{\bar{1},\bar{2},\bar{3},\bar{4},\bar{5},\bar{6}\}$，每个元素的阶均是 $\varphi(7)=6$ 的因子. 所以阶只能为 1, 2, 3 或 6

1阶元素：$\bar{1}$

2阶元素：$\overline{-1}=\bar{6}$

3阶元素：$\bar{2}$ 和 $\bar{4}$

6阶元素：$\bar{3}$ 和 $\bar{5}$

def 5.4 若整数 a 模 m 的阶为 $\varphi(m)$，称 a 是模 m 的原根

Thm 5.5 模 m 具有原根当且仅当 $m=2,4,p^\alpha$ 或 $2p^\alpha$，其中 p 为奇素数.

引理5.6 对每个奇素数 p，模 p 必有原根.

证：方法一：

Fermat小定理表明：$x^{p-1}-\bar{1}=0$ 在域 $\mathbb{Z}_p$ 中有 $p-1$ 个不同的解.

$\bar{1},\bar{2},\cdots,\overline{p-1}$ 考虑 $p-1$ 的标准分解式：

$$p-1=p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}$$

令 $p-1=n_i p_i^{a_i}$ $(1\le i\le s)$，则

$$x^{p-1}-\bar{1}=(x^{p_i^{a_i}}-\bar{1})f_i(x).$$

其中 $f_i(x)=x^{(n_i-1)p_i^{a_i}}+x^{(n_i-2)p_i^{a_i}}+\cdots+x^{p_i^{a_i}}+\bar{1}$ 是多项式，

其系数属于 $\mathbb{Z}_p$.

由 Lagrange 定理，l 次多项式在 $\mathbb{Z}_p$ 中至多有 l 个根.

由于 $x^{p-1}-\bar{1}$ 有 $p-1$ 个根，它们都是 $x^{p_i^{a_i}}-\bar{1}$ 的根或 $f_i(x)$ 的根

可知 $x_i^{p_i^{a_i}}-\bar{1}$ 在 $\mathbb{Z}_p$ 中必有 $p_i^{a_i}$ 个不同的根

这些根 $\alpha\in\mathbb{Z}_p^*$ 且 $\alpha^{p_i^{a_i}}=1$

若 α 的阶小于 $p_i^{a_i}$，则 $\alpha^{p_i^{a_i-1}}=\bar{1}$，即 α 是 $x^{p_i^{a_i-1}}-\bar{1}=0$ 的根

这样的 α 至多有 $p_i^{a_i-1}$ 个.

这表明对每个 $i\,(1\le i\le s)$，$\mathbb{Z}_p^*$ 中均有 $p_i^{a_i}$ 阶元素 α_i.

由于 $p_i^{a_i}\,(1\le i\le s)$ 两两互素，可知 $\alpha=\alpha_1\alpha_2\cdots\alpha_s$ 的阶为

$p_1^{a_1}p_2^{a_2}\cdots p_s^{a_s}=p-1$ （可自证）

令 $\alpha=\bar{a}\ (a\in\mathbb{Z})$，则 a 是模 p 的原根.

方法2：$\mathbb{Z}_p^*$ 中每个元素 α 的阶都是 $\varphi(p)=p-1$ 的正因子

对每个 $d\mid p-1$，以 N_d 表示 $\mathbb{Z}_p^*$ 中 d 阶元素的个数，则 $\sum_{d\mid p-1}N_d=p-1$

若 $N_d\ge1$，即 $\mathbb{Z}_p^*$ 中有 d 阶元素 α，则它是 $x^d-\bar{1}=0$ 的解.

但是 $1=\alpha^0,\alpha,\cdots,\alpha^{d-1}$ 是 $\mathbb{Z}_p^*$ 中 d 个不同的元素，它们均为 $x^d-\bar{1}=0$

的解.（$(\alpha^i)^d=(\alpha^d)^i=\bar{1}$），从而是 $x^d-\bar{1}=\bar{0}$ 在 $\mathbb{Z}_p^*$ 中的全部解.

这表明：$\mathbb{Z}_p^*$ 中每个 d 阶元素均有形式 α^i.

但 $\alpha^i\,(1\le i\le d)$ 的阶为 d 当且仅当 $(i,d)=1$

$\mathbb{Z}_p^*$ 中 d 阶元素若存在，则必有 $\varphi(d)$ 个，即 $N_d=0$ 或 $\varphi(d)$.

于是，$p-1=\sum_{d\mid p-1}N_d\le\sum_{d\mid p-1}\varphi(d)=p-1$

由于上式左右两边相同，这表明对每个 $d\mid p-1$，均为 $N_d=\varphi(d)$.

特别地，$N_{p-1}=\varphi(d-1)\ge1$，即 $\mathbb{Z}_p^*$ 中有 $p-1$ 阶元素，从而模 p 存在

原根.

注：对$p-1$的每个正因子d，$\mathbb{Z}_p^*$中d阶元素共有$\varphi(d)$个．特别地，模p共有$\varphi(p-1)$个原根（每个模p同余类看作是一个原根）．并且若g是模m的原根，则模p的全部$\varphi(p-1)$个原根为 g^i $(1\le i\le p-1,\ (i,p-1)=1)$

更一般地，对于$p-1$的每个正因子d，$\mathbb{Z}_p^*$中共有$\varphi(d)$个d阶元素，它们是（令$p-1=dl$） g^{ls} $(1\le s\le d,\ (s,d)=1)$

ex. $p=13$　$\varphi(p)=12$　由$2^6\equiv 64\not\equiv 1 \pmod{13}$

$2^4\equiv 16\not\equiv 1 \pmod{13}$　可知2是模13的一个原根．

于是：$\mathbb{Z}_{13}^*$中的12阶元素有$\varphi(12)=4$个：$\bar{2}$，$\bar{2}^5=\bar{6}$，$\bar{2}^7=\overline{11}$，$\bar{2}^{11}=\bar{7}$

6阶元素有$\varphi(6)=2$个：$\bar{2}^2=\bar{4}$ 和 $\bar{2}^{10}=\overline{10}$

4阶元素有$\varphi(4)=2$个：$\bar{2}^3=\bar{8}$ 和 $(\bar{2}^3)^{-1}=(\bar{8})^{-1}=\bar{5}$

3阶元素有$\varphi(3)=2$个：$\bar{2}^4=\bar{3}$，$(\bar{3})^{-1}=\bar{9}$

2阶元素有$\bar{-1}=\overline{12}$

1阶元素为$\bar{1}$．

引理5.7　设p为奇素数，$a\ge 2$，g是模p的原根．则g和$g+p$中必有一个是模p^a的原根

证：如果$g^{p-1}\not\equiv 1 \pmod{p^2}$　下证g是模p^a的原根

记g模p^a的阶为r，则$g^r\equiv 1 \pmod{p^a}$

$\therefore r \mid \varphi(p^a)=p^{a-1}(p-1)$

另一方面，由$g^r\equiv 1 \pmod{p^a}$ 可知 $g^r\equiv 1 \pmod{p}$

$\because g$是模p的原根　从而$\varphi(p)=p-1 \mid r$

$\therefore r=(p-1)p^t$　$0\le t\le a-1$　(1)

又$g^{(p-1)p^{a-2}}\not\equiv 1 \pmod{p^a}$　(2)

由假设$g^{p-1}\not\equiv 1 \pmod{p^2}$　可知(2)对$a=2$成立．

现假设(2)对$a=k$成立$(k\ge 2)$ 即 $g^{(p-1)p^{k-2}}\not\equiv 1 \pmod{p^k}$

再由$g^{(p-1)p^{k-2}}\equiv 1 \pmod{p^{k-1}}$　(Euler定理)

可知：$g^{(p-1)p^{k-2}}=1+p^{k-1}A$　$(A\in\mathbb{Z},\ p\nmid A)$

于是 $g^{(p-1)p^{k-1}} = (1+p^{k-1}A)^p \equiv 1+p^kA \not\equiv 1 \pmod{p^{k+1}}$

即〈2〉对 $a=k+1$ 成立.

由归纳假设知〈2〉对每个 $a\geq 2$ 均成立.

则证明了〈1〉中的 t：$t=a-1$ 即 g 为模 p^a 的原根 $(a\geq 2)$

若 $g^{p-1}\equiv 1 \pmod{p^2}$，则 $g^t = g+p$ 也是模 p 的原根.

并且 $g^{t\,p-1} \equiv (g+p)^{p-1} \equiv g^{p-1}+(p-1)p \equiv 1-p \not\equiv 1 \pmod{p^2}$

由以上推导可知：$g^t = p+g$ 是模 p^a 的原根.

引理 5.8 设 p 为奇素数，$a\geq 1$，则模 $2p^a$ 存在原根.

证：设 g 是模 p^a 的一个原根，则 g 和 $g+p^a$ 当中恰有一个为奇数.

记作 g'，则 $(g', 2p^a)=1$.

设 g' 模 $2p^a$ 的阶为 r，则 $(g')^r \equiv 1 \pmod{2p^a}$.

且 $r \mid \varphi(2p^a) = \varphi(p^a)$

由于 $(g')^r \equiv 1 \pmod{p^a}$，而 g' 为模 p^a 的原根

可知：$\varphi(p^a) \mid r$

于是，$r = \varphi(p^a) = \varphi(2p^a)$

从而 g' 是模 $2p^a$ 的原根

引理 5.9 设 $m\geq 2$，如果 $m\neq 2, 4, p^a$ 或 $2p^a$，其中 p 为奇素数，而 $a\geq 1$，则模 m 不存在原根.

证明：若 m 不是 $2, 4, p^a$ 或 $2p^a$，则 m 必可表示成

$$m = m_1 m_2,\quad (m_1, m_2)=1,\quad m_1\geq 3,\ m_2\geq 3$$

此时 $\varphi(m_1)$ 和 $\varphi(m_2)$ 均为偶数，从而

$$[\varphi(m_1), \varphi(m_2)] = 2\left[\frac{\varphi(m_1)}{2}, \frac{\varphi(m_2)}{2}\right] \leq 2\cdot\frac{\varphi(m_1)}{2}\cdot\frac{\varphi(m_2)}{2}$$

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

记 $A = [\varphi(m_1), \varphi(m_2)]$ 由 Euler 定理可知：

当 $(a, m)=1$ 时，$a^A \equiv 1 \pmod{m_1}$ 且 $a^A \equiv 1 \pmod{m_2}$

于是 $a^A \equiv 1 \pmod{m}$，但 $A < \varphi(m)$

∴ $\mathbb{Z}_m^*$ 中每个元素 a 的阶均小于 $\varphi(m)$，即模 m 不存在原根

(可以用原根来证明 Wilson 定理，也可用 Lagrange 定理来证明 Wilson 定理)

定理5.10 设$m\ge 2$，模m具有原根g，则对$\varphi(m)$的每个正因子d，$\mathbb{Z}_m^*$中共有$\varphi(d)$个d阶元素，它们是：$\bar{g}^{ld'}$ $(1\le l\le d,\ (l,d)=1)$，这里，$d'=\frac{\varphi(m)}{d}$

证：$\mathbb{Z}_m^*=\{1,\bar{g},\bar{g}^2,\cdots,\bar{g}^{\varphi(m)-1}\}$

对$0\le n\le\varphi(m)-1$，$\bar{g}^n$的阶为$\frac{\varphi(m)}{(\varphi(m),n)}$

∴当$dd'=\varphi(m)$时，有$\bar{g}^n$的阶为$d \Leftrightarrow (n,\varphi(m))=d'$

$\Leftrightarrow d'|n$ 且 $(\frac{n}{d'},d)=1 \Leftrightarrow n=ld',\ 1\le l\le d,\ (l,d)=1$

二、指数

设模m有原根g，则$\{1,g,g^2,\cdots,g^{\varphi(m)-1}\}$为模$m$的缩系

所以对每个与m互素的整数a，必存在唯一的整数k，使得：

$$a\equiv g^k \pmod m \quad 0\le k\le\varphi(m)-1$$

def 5.11 上述的k叫做a对于原根g的模m的指数(index)。表示成$\mathrm{ind}_g a$。当g固定时也简记为$k=\mathrm{ind}\, a$。

ex: $\mathrm{ind}\,1=0$ $\quad \mathrm{ind}_g g=1$ $\quad \mathrm{ind}(-1)=\frac{\varphi(m)}{2}$ $(m\ge 3)$

模m的指数与通常的对数有许多类似性质，所以$\mathrm{ind}_g a$也称做a的离散对数。

Thm 5.12 设$(a,m)=(b,m)=1$，则

1) $a\equiv b \pmod m$ 当且仅当 $\mathrm{ind}_g a=\mathrm{ind}_g b$.

2) $\mathrm{ind}(ab)\equiv\mathrm{ind}(a)+\mathrm{ind}(b) \pmod{\varphi(m)}$

$\mathrm{ind}(a^n)\equiv n\cdot\mathrm{ind}\,a \pmod{\varphi(m)}$ 对每个$n\in\mathbb{Z}$

证：1)可由定义直接得到

2)由于g模m的阶为$\varphi(m)$，所以

$$g^i\equiv g^j \pmod m \Leftrightarrow i\equiv j \pmod{\varphi(m)}$$

$$g^i\equiv a \pmod m \Leftrightarrow i\equiv \mathrm{ind}_g a \pmod{\varphi(m)}$$

于是 $g^{\mathrm{ind}(ab)}\equiv ab\equiv g^{\mathrm{ind}(a)}\cdot g^{\mathrm{ind}(b)}=g^{\mathrm{ind}(a)+\mathrm{ind}(b)} \pmod m$

因此 $\mathrm{ind}(ab)\equiv\mathrm{ind}\,a+\mathrm{ind}\,b \pmod{\varphi(m)}$。另一个同余式为上式推论

例1 $p=11$，2为模11的原根，以下将Z_{11}中的$\bar{a}$简记为a，从而$a=b$是指$a\equiv b \pmod{11}$，于是Z_{11}^*中元素为：

$2^0=1 \quad 2^1=2 \quad 2^2=4 \quad 2^3=8 \quad 2^4=5$

$2^5=10 \quad 2^6=9 \quad 2^7=7 \quad 2^8=3 \quad 2^9=6$

由此可列出模11（对于原根2）的"指数表"：

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{ind}_2 a$	0	1	8	2	4	9	7	3	6	5

利用指数概念可以解某些高次同余方程：

def 5.13 设$k\geq 2$，$(a,m)=1$，如果同余方程

$$x^k\equiv a \pmod m$$

有整数解，称a是模m的k次剩余，否则称a是模m的k次非剩余。

a是否为模m的k次剩余，这是模m同余类$\bar{a}$的性质。

当模m有原根时，同余方程$x^k\equiv a \pmod m$ (1) 的解有如下完整：

Thm 5.14 设$k\geq 2$，$(a,m)=1$，模m存在原根g，记$d=(k,\varphi(m))$，则

1) a为模m的k次剩余（即方程(1)有整数解）的充要条件为$d \mid \mathrm{ind}_g a$，这也相当于$a^{\frac{\varphi(m)}{d}}\equiv 1 \pmod m$

2) 若a为模m的k次剩余，则同余方程(1)模m恰有d个解。

3) 模m的k次剩余（类）a的个数为$\frac{\varphi(m)}{d}$，它们是

$$a\equiv g^{dl} \pmod m \quad (0\leq l\leq \frac{\varphi(m)}{d}-1)$$

证：1) 令 $x=g^y$，$a=g^{ind(a)}$，则同余方程(1)等价于

$$g^{ky}\equiv g^{ind(a)}\pmod m$$

这又等价于 $ky\equiv ind(a)\pmod{\varphi(m)}$

而该同余方程有解的充要条件是 $d=(k,\varphi(m))\mid ind_g(a)$

进而 $a^{\frac{\varphi(m)}{d}}\equiv g^{ind_g(a)\frac{\varphi(m)}{d}}\pmod m$

于是 $a^{\frac{\varphi(m)}{d}}\equiv 1\pmod m$

$\Leftrightarrow \varphi(m)\mid ind_g(a)\frac{\varphi(m)}{d}$

$\Leftrightarrow d\mid ind_g(a)$

2) 当 $d=(k,\varphi(m))\mid ind_g(a)$ 时，我们知道同余方程

$$ky\equiv ind_g(a)\pmod{\varphi(m)}$$

模 $\varphi(m)$ 有 d 个解 $y\equiv y_1,y_2,\cdots,y_d\pmod{\varphi(m)}$

于是同余方程(1)模 m 有 d 个解 $x\equiv g^{y_1},g^{y_2},\cdots,g^{y_d}\pmod m$

3) 由1)知：a 是模 m 的 k 次剩余当且仅当 $d\mid ind_g(a)$

所以 $ind_g(a)$ 模 $\varphi(m)$ 有 $\frac{\varphi(m)}{d}$ 个同余类：

$$ind_g(a)\equiv 0,d,2d,\cdots,\left(\frac{\varphi(m)-1}{d}-1\right)d\pmod{\varphi(m)}$$

于是模 m 的 k 次剩余共有 $\frac{\varphi(m)}{d}$ 个模 m 同余类：

$$a\equiv g^{dl}\pmod m\quad \left(0\le l\le \frac{\varphi(m)}{d}-1\right)$$

例：解同余方程：$7\cdot 3^x\equiv 6\pmod{11}$

解：方程等价于 $ind_2 7+x\cdot ind_2 3\equiv ind_2 6\pmod{10}$

查指数表可知：$7+8x\equiv 9\pmod{10}$

即 $8x\equiv 2\pmod{10}$

$\therefore x\equiv 4\pmod 5$