第4章 原根和指数

原根和指数

高次同余方程 $x^k \equiv a \pmod{n}$

4.1 原根

设$n \geq 1$，$(a,n)=1$，是否有正整数d使得$a^d \equiv 1 (\mathrm{mod}\, n)$？

定义 4.1.1 设$n \geq 1$，$(a,n)=1$，使得$a^d \equiv 1 (\mathrm{mod}\, n)$成立的最小正整数$d$，称为$a$对模$n$的阶，记作$\delta_n(a)$。

定理 4.1.1 设n为正整数，$(a,n)=1$，若$a^d \equiv 1 (\mathrm{mod}\, n)$，则$\delta_n(a) | d$。

推论 4.1.1 设n为正整数，$(a,n)=1$，则有$\delta_n(a) | \varphi(n)$。

定义 4.1.2 当$\delta_n(a)=\varphi(n)$时，称a是模n的原根。

例 1 $n=10$，取模 10 的一个缩系$\{1,3,7,9\}$， 因为

$$1^1 \equiv 1(\mathrm{mod}10);$$

$$3^2 \equiv 9(\mathrm{mod}10), 3^3 \equiv 7(\mathrm{mod}10), 3^4 \equiv 1(\mathrm{mod}10);$$

$$7^2 \equiv 9(\mathrm{mod}10), 7^3 \equiv 3(\mathrm{mod}10), 7^4 \equiv 1(\mathrm{mod}10);$$

$$9^2 \equiv 1(\mathrm{mod}10);$$

所以

$$\delta_{10}(1)=1, \delta_{10}(3)=4, \delta_{10}(7)=4, \delta_{10}(9)=2,$$

它们都是$\varphi(10)=4$的因子，且 3 和 7 均是模 10 的原根。

例 2 $n=8$，取模 8 的一个缩系$1,3,5,7$， 因为

$$1^1 \equiv 1(\mathrm{mod}8), 3^2 \equiv 1(\mathrm{mod}8), 5^2 \equiv 1(\mathrm{mod}8), 7^2 \equiv 1(\mathrm{mod}8),$$

所以

$$\delta_8(1)=1, \delta_8(3)=2, \delta_8(5)=2, \delta_8(7)=2,$$

而$\varphi(8)=4$，故而模 8 没有原根。

定理 4.1.2 (1) 若$a \equiv b(\mathrm{mod}\, n)$，$(a,n)=1$，则$\delta_n(a)=\delta_n(b)$。

(2) 若$(a,n)=1$，$a^k \equiv a^l(\mathrm{mod}\, n)$，则$k \equiv l(\mathrm{mod}\, \delta_n(a))$。

(3) 若$(a,n)=1$，则$1=a^0,a^1,\cdots,a^{\delta_n(a)-1}$这$\delta_n(a)$个数模$n$两两不同余，特别当$a$是模$n$的原根时，这$\delta_n(a)=\varphi(n)$个数是模$n$的一组缩系。

(4) 设a^{-1}是a模n的逆，则$\delta_n(a^{-1})=\delta_n(a)$。

例 3 求$\delta_{11}(3)$和$\delta_{11}(2)$。

解：由定理 4.1.1，$\delta_{11}(3)\mid\varphi(11)=10$，故只需对 10 的因子 1,2,5,10 进行验证。因为

$$3^1\equiv 3(\mathrm{mod}11)，\ 3^2\equiv 9(\mathrm{mod}11)，\ 3^5\equiv 243\equiv 1(\mathrm{mod}11)，$$

所以$\delta_{11}(3)=5$。

同理，因为

$$2^1\equiv 2(\mathrm{mod}11)，\ 2^2\equiv 4(\mathrm{mod}11)，\ 2^5\equiv 32\equiv 10(\mathrm{mod}11)，$$

$$2^{10}\equiv 1(\mathrm{mod}11)，$$

所以$\delta_{11}(2)=10=\varphi(11)$，即 2 是模 11 的一个原根。

考察

$$2^0,\ 2^1,\ 2^2,\ 2^3,\ 2^4,\ 2^5,\ 2^6,\ 2^7,\ 2^8,\ 2^9,$$

确为模 11 的一个缩系，同余于

$$1,\ 2,\ 4,\ 8,\ 5,\ 10,\ 9,\ 7,\ 3,\ 6。$$

定理 4.1.3 设$n=2^l p_1^{l_1}\cdots p_s^{l_s}$，其中$l\geq 0, l_i\geq 1$，而$p_1,\cdots,p_s$是不相同的奇素数，则

(1) 当$l\geq 2$并且$n\neq 4$时，模n没有原根；

(2) 当$s\geq 2$时，模n没有原根。

证明：构造一个严格小于$\varphi(n)$的整数x，使得对任意$(a,n)=1$有

$$a^x\equiv 1(\mathrm{mod}\, n)。$$

(1) 令$n=2^l m$，其中m为奇数。分别讨论$l=2$和$l\geq 3$的情形。对$l\geq 3$的情形需要利用$a^{2^{l-2}}\equiv 1(\mathrm{mod}\, 2^l)$，可数学归纳法证明。

(2) $s\geq 2$时，可取正整数n_1,n_2，使得$n=n_1n_2$，而n_1,n_2均含奇素因子并且$(n_1,n_2)=1$。利用$\varphi(n_1)$和$\varphi(n_2)$均为偶数来完成证明。

定理 4.1.3 告诉我们，若模n存在原根，则

$$n=2,4,p^l,2p^l,$$

其中p为奇素数，$l\in N^+$.

对$n=2,4,p^l,2p^l$是否一定存在原根却不得而知。

对$n=2,4$，我们容易验证$1,-1$分别是模 2 和模 4 的原根

定理 4.1.4 设$(a,n)=1$，则a^k对模n的阶为$\dfrac{\delta_n(a)}{(k,\delta_n(a))}$，特别有$a^k$对模$n$的阶为$\delta_n(a)$的充分必要条件是$(k,\delta_n(a))=1$，从而$1,\ a,\ \cdots,\ a^{\delta_n(a)-1}$中共有$\varphi(\delta_n(a))$个数对模$n$的阶为$\delta_n(a)$，特别地，若模$n$有原根，则原根共有$\varphi(\varphi(n))$个。

例 4 设$n=11$，则$\varphi(11)=10$的所有因子为 1,2,5,10。由

$2^1\equiv 2(\mathrm{mod}11), 2^2\equiv 4(\mathrm{mod}11),\ 2^5\equiv 10(\mathrm{mod}11), 2^{10}\equiv 1(\mathrm{mod}11),$

可知$g=2$为模 11 的一个原根。

根据定理 4.1.4，模 11 的一个缩系中，对于 10 的每个正因子d，g^i模 11 阶为d的充分必要条件是$d=\dfrac{10}{(i,10)}$，因此

模 11 阶为 1 的有$\varphi(1)=1$个，它是$2^{10}(i=10)$，即 1；

模 11 阶为 2 的有$\varphi(2)=1$个，它是$2^5(i=5)$，即 10；

模 11 阶为 5 的有$\varphi(5)=4$个，它是$2^2,2^4,2^6,2^8(i=2,4,6,8)$，即 4，5，9，3；

模 11 阶为 10 的有$\varphi(10)=4$个，它是$2^1,2^3,2^7,2^9(i=1,3,7,9)$，即 2，8，7，6；

$\varphi(11)=10$，所以模 11 的原根为$2^1,2^3,2^7,2^9$，即 2，8，7，6。

定理 4.1.5 对于每个素数 p，均存在模 p 的原根。

引理 **4.1.6** 设 p 为奇素数，若整数 u 满足 $u^{p-1}=1+t_1 p$，其中整数 $t_1 \not\equiv 0 (\mathrm{mod}\ p)$，则 $u^{\varphi(p^l)}=1+t_l p^l$，其中 $t_l \not\equiv 0 (\mathrm{mod}\ p)$。

推论 4.1.6 设 p 为奇素数，若整数 u 满足 $u^{p-1}=1+t_1 p$，其中整数 $t_1 \not\equiv 0 \pmod{p}$，则 $\forall n \in N^+$ 有

$$u^{\varphi(p^n)} \equiv 1 \pmod{p^n},$$

而 $$u^{\varphi(p^n)} \not\equiv 1 \pmod{p^{n+1}}。$$

引理 **4.1.6′** 设g_0为模p的一个原根，则$\forall t \in Z$，$n \in N^+, g_0 + tp$模p^n的阶δ满足

(1) $\delta \mid \varphi(p^n)$；

(2) $(p-1) \mid \delta$。

定理 4.1.6 设 p 为奇素数，$l \geq 2, l \in N^+$，模 p^l 必有原根。

例 5 求模11^4的一个原根。

解：利用定理 4.1.6 的证明知，$g_0 = g + 11t_0$为模11^4的一个原根，其中

$$g \text{ 为模 } 11 \text{ 的一个原根，}$$

$$m + (11-1)g^{11-2}t_0 \not\equiv 0 (\mathrm{mod} 11),$$

$$k \text{ 满足 } g^{11-1} = 1 + 11m \text{。}$$

取$g = 2$，由

$$2^{10} = 1 + 11 \times 93$$

知$m = 93$。

取$93 + 10 \cdot 2^9 t \not\equiv 0 (\mathrm{mod} 11)$的一个解

$$t_0 = 1,$$

则

$$g_0 = 2 + 11 \times 1 = 13$$

是模11^4的一个原根。

定理 4.1.7 设 p 为奇素数，g_0 为模 $p^l(l \in N^+)$ 的原根，则 $g_0, g_0 + p^l$ 中必有一个为奇数，且这个奇数就是模 $2p^l$ 的原根。

例 6 2 为模 3 的原根，由于

$$2^{3-1}\equiv 1+3\times 1(\mathrm{mod}\,3^2),1\not\equiv 0(\mathrm{mod}\,3),$$

所以由定理 4.1.6 的证明知 2 亦为模$3^l(l\geq 2)$的原根。

又由定理 4.1.7 知

$$2+3=5$$

为模$2\times 3=6$的原根，

$$2+3^2=11$$

为模$2\times 3^2=18$的原根。

定理 4.1.8 设n为正整数，则

模n有原根$\Leftrightarrow n=1,2,4,p^l,2p^l$，其中$p$为奇素数，$l\in N^+$。

若模n有原根，则原根共有$\varphi(\varphi(n))$个。

如果g是模n的一个原根，那么模n的全部原根为

$$\{g^i \mid 1\le i\le \varphi(n),(i,\varphi(n))=1\},$$

我们还可记$g^i=g_i$，这时$\forall 1\le i\le \varphi(n),(i,\varphi(n))=1$

$$g_i^{\,0},\ g_i^{\,1},\ \cdots,\ g_i^{\,\varphi(n)-1}$$

均构成模n的缩系。

例 7 求模 43 的原根。

解：43 是一个素数，我们通过试算来求解它的原根。

$\varphi(43)=42=2\times3\times7$，其因子 d=1,2,3,6,7,14,21,42。

先求 2 模 43 的阶：因为

$$2^2\equiv4(\mathrm{mod}\,43)\ ,\quad 2^3\equiv8(\mathrm{mod}\,43)\ ,\quad 2^6\equiv21(\mathrm{mod}\,43)\ ,$$

$$2^7\equiv-1(\mathrm{mod}\,43),\quad 2^{14}\equiv1(\mathrm{mod}\,43),$$

所以$\delta_{43}(2)=14$。

再求 3 模 43 的阶：同样，因为

$$3^2\equiv9(\mathrm{mod}\,43)\ ,\quad 3^3\equiv-16(\mathrm{mod}\,43)\ ,\quad 3^4\equiv-5(\mathrm{mod}\,43)\ ,$$

$$3^{14}\equiv-7(\mathrm{mod}\,43),\quad 3^{21}\equiv-1(\mathrm{mod}\,43),$$

所以$\delta_{43}(3)=42$，即 3 为模 43 的一个原根。

由此及定理 4.1.8，模 43 的所有原根为

$$\{3^i\,|\,1\le i\le42,(i,42)=1\}。$$

在例 7 的基础之上，我们还可以求模$43^l, 2\cdot 43^l (l>1)$的原根。

先求3^{42}对模$43^2 = 1849$的剩余，并将之表示成$1+k\cdot 43$的形式。具体步骤如下：

由于$43 \nmid 2$，所以 3 为模43^l的原根。

又 3 为奇数，由定理 4.1.7 知 3 亦为模$2\cdot 43^l$的原根。

4.2 指数

当模n有原根g时，

$$1, g^1, \cdots, g^{\varphi(n)-1}$$

为模n的一个缩系，从而对每个与n互素的整数a，必定存在唯一的整数$k(0 \le k < \varphi(n))$，使得

$$a \equiv g^k \pmod{n}。$$

这样以来，当模n有原根g时，通过原根g，

模n的缩系

与

模$\varphi(n)$的完系

之间就建立了一一对应。

定义 4.2.1 整数k叫作a对模n以原根g为底的指数，如果$a \equiv g^k \pmod{n}$并且$0 \le k < \varphi(n)$，其中$(a,n)=1, n \in N^+$。记作$k = ind_g a$，在不混淆的情况下，可简记为$inda$。

例 1 模$n=11$，$g=2$是模 11 的一个，则$2^0, 2^1, \cdots, 2^{10-1}$为模 11 的缩系。由

$$1 \equiv 2^0 \pmod{11}, \quad 2 \equiv 2^1 \pmod{11},$$
$$4 \equiv 2^2 \pmod{11}, \quad 8 \equiv 2^3 \pmod{11},$$
$$5 \equiv 2^4 \pmod{11}, \quad 10 \equiv 2^5 \pmod{11},$$
$$9 \equiv 2^6 \pmod{11}, \quad 7 \equiv 2^7 \pmod{11},$$
$$3 \equiv 2^8 \pmod{11}, \quad 6 \equiv 2^9 \pmod{11}$$

可以得到 1,2,3,4,5,6,7,8,9 对模 11 以 2 为底的指数。为清楚起见，我们将其列表如下：

指数表

a	1	2	3	4	5	6	7	8	9	10
$ind_2(a)$	0	1	8	2	4	9	7	3	6	5

定理 4.2.1 设g是模n的原根，$(a,n)=(b,n)=1$，则

(1) $g^{ind_g a} \equiv a(\mathrm{mod}\, n)$；

(2) $g^h \equiv g^k(\mathrm{mod}\, n) \Leftrightarrow h \equiv k(\mathrm{mod}\, \varphi(n))$；

(3) $ind_g(ab) \equiv ind_g a + ind_g b(\mathrm{mod}\, \varphi(n))$；

(4) 对每个正整数m有$ind_g(a^m) \equiv m \cdot ind_g a(\mathrm{mod}\, \varphi(n))$。

给定$n, g, ind_g(a)$时，可以利用快速指数算法计算出

$$a = g^{ind_g(a)} (\mathrm{mod}\, n),$$

但是给定n, g, a时，要计算相应指数$ind_g(a)$则非常困难。

这就是所谓的离散对数问题。

定理 4.2.2 设g_1, g_2是模n的两个不同的原根，$(a,n)=1$，则

$$ind_{g_2} a \equiv (ind_{g_2} g_1)\cdot(ind_{g_1} a)(\mathrm{mod}\,\varphi(n))。$$

定理 4.2.3 设g是模n的原根，$(\alpha,n)=1$，则$\delta_n(\alpha)=\dfrac{\varphi(n)}{(ind_g\alpha,\varphi(n))}$。

定理 4.2.4 设g为模n的一个原根，$d>0, d \mid \varphi(n)$，则模n以d为阶的整数为：

$$g^{i\left(\frac{\varphi(n)}{d}\right)} (\mathrm{mod}\, n)$$，其中$1 \le i \le d, (i,d)=1$；

这就意味着在模n的一个缩系中，以d为阶的元素有$\varphi(d)$个。

定义 4.2.2 设$(a,n)=1$，$k\geq 2$. 如果同余方程$x^k\equiv a(\mathrm{mod}\,n)$有解，则称$a$是模$n$的$k$次剩余；否则称$a$是模$n$的$k$次非剩余。

定理 4.2.5 设模n存在原根，$k\geq 2$，g是模n的一个原根，$(a,n)=1$，则

(1) 同余方程$x^k\equiv a(\mathrm{mod}\,n)$有解

$$\Leftrightarrow (k,\varphi(n))\,|\,ind_g(a)\Leftrightarrow a^{\frac{\varphi(n)}{(k,\varphi(n))}}\equiv 1(\mathrm{mod}\,n);$$

(2) 若(1)中条件成立时，则同余方程$x^k\equiv a(\mathrm{mod}\,n)$模$n$共有$(k,\varphi(n))$个解；

(3) 模n的缩系中恰有$\dfrac{\varphi(n)}{(k,\varphi(n))}$个$k$次剩余。

例 2 解同余方程 $x^8 \equiv 38 (\mathrm{mod}11)$。

解：不难验证 2 是模 11 的一个原根，由例 1 中模 11 的指数表

a	1	2	3	4	5	6	7	8	9	10
$ind_2(a)$	0	1	8	2	4	9	7	3	6	5

及 $38 \equiv 5(\mathrm{mod}11)$ 易知

$$ind_2 38 = ind_2 5 = 4,$$

故原同余方程等价于

$$8ind_2 x \equiv 4(\mathrm{mod}10),$$

因为 $(8,10) = 2 \mid 4$，所以该一次同余方程模 10 有两个解，易知其解为

$$ind_2 x \equiv 3,8(\mathrm{mod}10),$$

再由例 1 中的指数表可查得 $x \equiv 8,3(\mathrm{mod}11)$，这就是原同余方程的解。

例 3 解同余方程$6\cdot 8^x \equiv 9(\mathrm{mod}13)$。

解：易验证 2 是模 13 的一个原根，构造指数表如下：

a	1	2	3	4	5	6	7	8	9	10	11	12
$ind_2 a$	0	1	4	2	9	5	11	3	8	10	7	6

由此原同余方程可化为

$$ind_2 6 + x\cdot ind_2 8 \equiv ind_2 9(\mathrm{mod}12),$$

$$5+3x \equiv 8(\mathrm{mod}12),$$

易知$x \equiv 1(\mathrm{mod}\,4)$为上述同余方程的解，从而

$$x \equiv 1(\mathrm{mod}\,4)(x \geq 0)$$

为原同余方程的解。