第6章 原根和指标

6.1 指数和原根

6.2 指标与二项同余方程

习题

6.1 指数和原根

6.1 指数和原根

在模指数运算 $a^d \bmod m$（其中 $(a,m)=1$）中，如果知道周期 d_0，使得 $a^{d_0} \equiv 1 \bmod m$，则使得计算简单。由Euler定理知这样的 d_0 一定存在 $(d_0=\varphi(n))$，但这个周期不一定是最小周期。关于最小周期有以下定义。

定义1.1 设 $m \in N$，$(a,m)=1$，使得 $a^d \equiv 1 \bmod m$ 成立的最小正整数 d 称为 a 对模 m 的指数（或阶），记为 $\delta_m(a)$。若 $\delta_m(a)=\varphi(m)$，称 a 是模 m 的原根。

例1.1 $m=7$，$\varphi(7)=6$ ，将模7的绝对最小简化剩余系中元素的指数列表如下（称为模7的指数表）

表6.1 模7的指数表

a	-3	-2	-1	1	2	3
$\delta_7(a)$	3	6	2	1	3	6

可见-2，3为原根。

例1.2 $m=10=2\cdot5$，$\varphi(10)=4$，模10的指数表是：

表6.2 模10的指数表

a	-3	-1	1	3
$\delta_{10}(a)$	4	2	1	4

可见 是原根。

例1.3 $m=9=3^2$，$\varphi(9)=6$，模9的指数表是：

表6.3 模9的指数表

a	-4	-2	-1	1	2	4
$\delta_9(a)$	6	3	2	1	6	3

可见-4 ， 2是原根。

例1.4 $m=8=2^3$，$\varphi(8)=4$，模8的指数表是：

表6.4 模8的指数表

a	-3	-1	1	3
$\delta_8(a)$	2	2	1	2

可见无原根。

指数有以下性质：

定理1.1 设 $m \in N, (a,m)=1$，若 $a^d \equiv 1 \bmod m$，则 $\delta_m(a) | d$

证明 由带余数除法，存在唯一的 q, r，使得 $d = q \cdot \delta_m(a) + r$ 其中 $0,, r < \delta_m(a)$，$a^d \equiv (a^{\delta_m(a)})^q \cdot a^r \equiv a^r \equiv 1$，由 $\delta_m(a)$ 的最小性知 $r = 0$。 证毕。

由Euler定理及定理1.1得：

推论 设 $m \in N$，$(a,m)=1$，则 $\delta_m(a) | \varphi(m)$。

由推论知在求 $\delta_m(a)$时，只需要在 $\varphi(m)$的因子中找。

例1.5 求 $\delta_{17}(5)$ 。

解 $\varphi(17)=16$，所以 $\delta_{17}(5)$ 只需在16的因子1，2，4，8，16中求。$5^1 \equiv 5$，$5^2 \equiv 25 \equiv 8$，$5^4 \equiv 64 \equiv 13 \equiv -4$，$5^8 \equiv 16 \equiv -1$，$5^{16} \equiv 1$，所以 $\delta_{17}(5)=16$。

定理1.2 设 $m \in N$ ，$(a,m)=1$ 。

（1） 若 $a \equiv b \bmod m$ ，则 $\delta_m(a)=\delta_m(b)$ ；

（2） 若 $a^k \equiv a^l \bmod m$，则 $k \equiv l \bmod \delta_m(a)$ ；

（3） $a^0=1, a^1, \cdots, a^{\delta_m(a)-1}$ 两两不同余；特别地当 a 是模 m 的原根时，构成了模 m 的一个简化剩余系；

（4） 设 a^{-1} 是 a 的逆，即 $a^{-1}a \equiv 1 \bmod m$，则 $\delta_m(a^{-1})=\delta_m(a)$

证明

（1）$a \equiv b \bmod m$，$(b,m)=(a,m)=1$。$b^{\delta_m(a)} \equiv a^{\delta_m(a)} \equiv 1 \bmod m$

由定理1.1，$\delta_m(b) \mid \delta_m(a)$。同理 $\delta_m(a) \mid \delta_m(b)$，所以

$\delta_m(a)=\delta_m(b)$。

（2）不妨设 $k \ldots l$，由 $a^k \equiv a^l \bmod m$ 得 $a^{k-l} \equiv 1 \bmod m$

由定理1.1，$\delta_m(a) \mid k-l$，即 $k \equiv l \bmod \delta_m(a)$。

（3） 若 $a^k \equiv a^l \bmod m$，其中 $0 \le k, l \le \delta_m(a)-1$，由(2)得 $k \equiv l \bmod \delta_m(a)$，所以 $k=l$。当 a 是模 m 的原根时，$\delta_m(a)=\varphi(m)$，$a^0=1, a^1, \cdots, a^{\delta_m(a)-1}$ 有 $\varphi(m)$ 个两两不同余的元素，因此构成了模 m 的一个简化剩余系。

（4）由 $a^{-1}a \equiv 1 \bmod m$，

$(a^{-1}a)^{\delta_m(a)} = (a^{-1})^{\delta_m(a)} a^{\delta_m(a)} = (a^{-1})^{\delta_m(a)} \equiv 1 \bmod m$，所以 $\delta_m(a^{-1}) \mid \delta_m(a)$，同理 $\delta_m(a) \mid \delta_m(a^{-1})$，所以 $\delta_m(a^{-1}) = \delta_m(a)$。

证毕。

例1.6 （第3章例1.1），2009年2月4日是星期一，问第2^{2018}天是星期几？

解 因为$(2,7)=1$，$\delta_7(2)=3$，$2018\equiv 2 \bmod \delta_7(2)$，所以$2^{2018}\equiv 2^2 \bmod 7\equiv 4 \bmod 7$，即第$2^{2018}$天是星期五。

定理1.3 设 $(a,m)=1$，k是非负整数，则 $\delta_m(a^k)=\dfrac{\delta_m(a)}{(k,\delta_m(a))}$。

证明 设 $\delta_m(a^k)=\delta'$，则

$$(a^k)^{\delta'}\equiv 1 \bmod m \Leftrightarrow a^{k\delta'}\equiv 1 \bmod m \Leftrightarrow \delta_m(a)\mid k\delta' \Leftrightarrow$$

$$\frac{\delta_m(a)}{(k,\delta_m(a))}\mid \frac{k}{(k,\delta_m(a))}\delta' \Leftrightarrow \frac{\delta_m(a)}{(k,\delta_m(a))}\mid \delta'$$，其中最后一个等价关系由 $\left(\dfrac{\delta_m(a)}{(k,\delta_m(a))},\dfrac{k}{(k,\delta_m(a))}\right)=1$ 得。所以最小的 δ'即为 $\dfrac{\delta_m(a)}{(k,\delta_m(a))}$。

证毕。

推论1 设 k是非负整数，g是模m的原根，则 g^k也是模m的原根的充要条件是 $(k,\varphi(m))=1$ 。

证明 $\delta_m(g^k)=\dfrac{\delta_m(g)}{(k,\delta_m(g))}=\dfrac{\varphi(m)}{(k,\varphi(m))}$ ，所以 $\delta_m(g^k)=\varphi(m)$ 当且仅当 $(k,\varphi(m))=1$ 。 证毕。

推论2 在 $1, a, \cdots, a^{\delta_m(a)-1}$ 中共有 $\varphi(\delta_m(a))$ 个数模 m 的指数为 $\delta_m(a)$ 。特别地，如果 a 是原根时，简化剩余系 $1, a, \cdots, a^{\varphi(m)-1}$ 中有 $\varphi(\varphi(m))$ 个原根。

证明 由定理1.3，$\delta_m(a^k) = \dfrac{\delta_m(a)}{(k, \delta_m(a))} = \delta_m(a)$，所以 $(k, \delta_m(a)) = 1$ 这样的 k 有 $\varphi(\delta_m(a))$ 个。

如果 a 是原根，即 $\delta_m(a) = \varphi(m)$，由定理1.2的（3），$1, a, \cdots, a^{\varphi(m)-1}$ 是模 m 的简化剩余系，其中指数为 $\varphi(m)$ 的元素有 $\varphi(\varphi(m))$ 个。 证毕。

例1.7 设 $m=11$，则 $\varphi(11)=10$，它的所有因子为1，2，5，10。由 $2^1\equiv 2 \bmod 11$，$2^2\equiv 4 \bmod 11$，$2^5\equiv 10 \bmod 11$，$2^{10}\equiv 1 \bmod 11$，知 $g=2$ 是模11的一个原根，模11的简化剩余系中每一元素 a 都可以写成2的幂。设 $a=2^k$，则 $\delta_{11}(a)=\dfrac{\delta_{11}(2)}{(k,\delta_{11}(2))}=\dfrac{10}{(k,10)}$，由定理1.1的推论知 $\delta_{11}(a)$ 是 $\varphi(11)=10$ 的因子。

若 $\delta_{11}(a)=1$，则 $(k,10)=10$，$k=10$，即指数为1的元素有1个：$2^{10}\equiv 1 \bmod 11$。

若 $\delta_{11}(a)=2$，则 $(k,10)=5$，$k=5$，即指数为2的元素有1个：$2^5\equiv 10 \bmod 11\equiv -1 \bmod 11$。

若 $\delta_{11}(a)=5$，则 $(k,10)=2$，$k=2,4,6,8$，即指数为5的元素有4个：$2^2\equiv 4 \bmod 11$，$2^4\equiv 5 \bmod 11$，$2^6\equiv 9\equiv -2 \bmod 11$，$2^8\equiv 3 \bmod 11$。

若 $\delta_{11}(a)=10$，则 $(k,10)=1$，$k=1,3,7,9$，即指数为10的元素有4个：$2^1\equiv 2 \bmod 11$，$2^3\equiv 8 \bmod 11\equiv -3 \bmod 11$，$2^7\equiv 7 \bmod 11\equiv -4 \bmod 11$，$2^9\equiv -5 \bmod 11$。

定理1.4 设$\delta_m(a)=s$，$\delta_m(b)=t$，$\delta_m(ab)=st$ 的充要条件是$(s,t)=1$。

证明 **充分性：**设$\delta=\delta_m(ab)$，$1=(ab)^{\delta}\equiv(ab)^{\delta t}=a^{\delta t}b^{\delta t}=a^{\delta t}$所以$s\mid\delta t$，但$(s,t)=1$，所以$s\mid\delta$。同理$t\mid\delta$，所以$st=[s,t]\mid\delta$又$(ab)^{st}=a^{st}b^{st}=1$，所以$\delta\mid st$，所以$\delta=st$。

必要性：$(ab)^{[s,t]}=a^{[s,t]}\cdot b^{[s,t]}=1$，所以$\delta_m(ab)=st\mid[s,t]$，由第1章定理2.14的（5），$(s,t)[s,t]=st$，$[s,t]\mid st$，所以$[s,t]=st$，$(s,t)=1$。 证毕。

定理1.5 设 $m=2^{\alpha}p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，其中 $\alpha \ldots 0$ ，$\alpha_i \geqslant 1(1 \leqslant i \leqslant s)$，$p_1,\cdots,p_s$ 是互不相同的奇素数，则

（1）当 $\alpha \ldots 2$ 且 $m \neq 4$ 时，模 m 没有原根。

（2）当 $s \ldots 2$ 时，模 m 没有原根。

证明 （1）当$\alpha=2$且$m\neq 4$时，则$m=4n$，其中$n>1$为奇数。由$(-1,n)=1$及Euler定理，$(-1)^{\varphi(n)}\equiv 1 \bmod n$，所以$\varphi(n)$为偶数。设$\varphi(n)=2k$，$k\in N$，则当$(g,m)=1$，有$(g,4)=1$且$(g,n)=1$。所以$g^{\varphi(4)}\equiv g^2\equiv 1 \bmod 4$，$g^{\varphi(n)}\equiv g^{2k}\equiv 1 \bmod n$。由$g^2\equiv 1 \bmod 4$得$g^{2k}\equiv 1 \bmod 4$。再由第3章定理1.9，$g^{2k}\equiv 1 \bmod (4n)\equiv 1 \bmod m$。但因$\varphi(m)=\varphi(4)\varphi(n)=2(2k)=4k>2k$，$g$不是原根，从而没有模$m$的原根。

当 $\alpha \geqslant 3$ 时，令 $m = 2^{\alpha} n$，其中 n 为奇数。当 $(g, n) = 1$ 时，由归纳法可证 $g^{2^{\alpha-2}} \equiv 1 \bmod 2^{\alpha}$。所以

$g^{2^{\alpha-2} \cdot \varphi(n)} \equiv (g^{2^{\alpha-2}})^{\varphi(n)} \equiv 1 \bmod 2^{\alpha}$，又 $g^{2^{\alpha-2} \cdot \varphi(n)} \equiv (g^{\varphi(n)})^{2^{\alpha-2}} \equiv 1 \bmod n$

由第3章定理1.9 $g^{2^{\alpha-2} \varphi(n)} \equiv 1 \bmod (2^{\alpha} n) \equiv 1 \bmod m$。但

$$\varphi(m) = \varphi(2^{\alpha}) \varphi(n) = (2^{\alpha} - 2^{\alpha-1}) \varphi(n) = 2^{\alpha-1} \varphi(n) > 2^{\alpha-2} \varphi(n),$$

所以 g 不是模 m 的原根，从而没有模 m 的原根。

（2）若 $s \geqslant 2$，可将 m 分解为 $m = m_1 m_2$，其中 m_1, m_2 均含奇素因子且 $(m_1, m_2) = 1$。由于 $\varphi(m_1), \varphi(m_2)$ 均为偶数，可设 $\varphi(m_1) = 2k_1, \varphi(m_2) = 2k_2$，则当 $(g, m) = 1$，$g^{2k_1} \equiv 1 \bmod m_1$ $g^{2k_2} \equiv 1 \bmod m_2$，从而 $g^{2k_1 k_2} \equiv 1 \bmod m_1$，$g^{2k_1 k_2} \equiv 1 \bmod m_2$，由第3章定理1.9，$g^{2k_1 k_2} \equiv 1 \bmod (m_1 m_2) \equiv 1 \bmod m$。但 $\varphi(m) = \varphi(m_1)\varphi(m_2) = 4k_1 k_2 > 2k_1 k_2$，$g$ 不是原根，从而没有模 m 的原根。 证毕。

推论 模m存在原根的必要条件是$m=1,2,4,p^{\alpha},2p^{\alpha}$，其中$\alpha\geqslant 1$是整数，$p$是奇素数。

反过来考虑满足推论的m是否一定存在原根，$m=1,2,4$分别有原根$1,1,-1$。下面讨论$m=p^{\alpha}$或$2p^{\alpha}$时是否有原根。

定理1.6（补充） 若p是奇素数, 则模p的原根是存在的。

证明2： 在模p的既约（简化）剩余系$1, 2, \cdots, p-1$里，每一整数对模p都有它自己的指数, 从这$p-1$个指数中取出所有不同的指数, 记作

$$\delta_1, \delta_2, \cdots, \delta_r \qquad (1)$$

令$\tau = [\delta_1, \delta_2, \cdots, \delta_r]$，则需要证明：

（Ⅰ）有一数g, 它对模p的指数是τ;

（Ⅱ）$\tau = p-1$

如果这两点被证明了, 那么g便是模p的一个原根而定理获证

注：补充的定理1.6, 1.7, 1.8，即初等数论（闵嗣鹤，严士健，第四版）定理1, 2, 3，P87-88页

证明2（续）：（Ⅰ）设$\tau = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_k^{\alpha_k}$ 是τ的标准分解式, 则对每一$s(s = 1, 2, \cdots, k)$来说, 在(1)里一定有一δ使得 $\delta = aq_s^{\alpha_s}$. 由(1)的意义知有一整数, 它对模p的指数是δ. 设这个整数是x, 则由定理1. 3知$x_s = x^{\mathrm{a}}$对模p的指数是$q_s^{\alpha_s}$. 故在$1, 2, \cdots, p-1$里有k个数$x'_1, x'_2, \cdots, x'_k$, 使x'_{s} $(s = 1,2, \cdots, \mathrm{k})$对模$p$的指数是$q_s^{\alpha_s}$. 令$\mathrm{g} = x'_1 x'_2 \cdots x'_k$, 则由定理6. 1. 4即知g对模$p$的指数是$\tau$

（Ⅱ）因为$\delta_{\mathrm{s}}(s = 1,2, \cdots, \mathrm{r})$是$\tau$的因数, 而$1, 2, \cdots, p-1$中任一数的指数都在(1)中出现, 故$x^{\tau} \equiv 1(mod\ p), x = 1,2, \cdots, p-1$,即同余式$x^{\tau} \equiv 1(mod\ p)$至少有$p-1$个解. 由第四章§4定理4知$p - 1 \leq \tau$. 但由§1推论1知$\delta_s | (p-1)$,s=1,2,$\cdots, r$, 故$\tau | (p-1)$. 由此即得$\tau \leq p-1$. 故$\tau = p-1$. 证完.

定理1.7 （补充） 设g是p的一个原根, 则存在一整数t_0, 使得由等式$(g+pt_0)^{p-1}=1+pu_0$, 所确定的u_0不能被p整除, 并且对应于这个t_0的$g+pt_0$就是模p^α的原根, 其中α是大于1的任何整数. **即对任一正整数α来说, 模p^α的原根存在.**

证明： 由欧拉定理即得$g^{p-1}\equiv 1(mod\ p)$, 也就是说存在一整数T_0, 使得下列两等式成立：

$$g^{p-1}=1+pT_0$$

$$(g+pt)^{p-1}=1+p(T_0-g^{p-2}t+pT)=1+pu \qquad (2)$$

其中$u=T_0-g^{p-2}t+pT$, T是t的整系数多项式. 显然对任何整数t来说, $u\equiv T_0-g^{p-2}t(mod\ p)$. 又由(2), $(g^{p-2},p)=1$. 故此时同余式$g^{p-2}t-T_0\equiv 0(mod\ p)$只有一解, 因而存在一$t_0$, 使$g^{p-2}t-T_0\not\equiv 0(mod\ p)$.故$t_0$所对应的$u_0$（即由$(g+pt_0)^{p-1}=1+pu_0$所确定的$u_0$ ）不被p整除.

证明（续）：对于满足上述要求的那个t_0, 我们还有

$$(\mathrm{g}+pt_0)^{p(p-1)}=(1+pu_0)^p=1+p^2u_1 \ (3)$$

其中

$$u_1=u_0+\binom{p}{2}u_0^2+\binom{p}{3}u_0^3+\cdots+p^{p-2}u_0^p\equiv u_0(mod\ p)$$

因而p不能整除u_1. 同样可得

$$(\mathrm{g}+pt_0)^{p^2(p-1)}=(1+p^2u_1)^p=1+p^3u_2$$

$$(\mathrm{g}+pt_0)^{p^3(p-1)}=(1+p^3u_2)^p=1+p^4u_3 \ (4)$$

$$\cdots$$

其中$u_0\equiv u_1(mod\ p)\equiv u_2(mod\ p)\equiv u_3(mod\ p)\equiv\cdots$,

即$p\nmid u_s, s=1,2,3,\cdots$.

证明（续）：

设$\mathrm{g}+pt_0$对模p^α的指数是δ，则

$$(\mathrm{g}+pt_0)^\delta \equiv 1(mod\ p^\alpha)\ (5)$$

由此即得$(\mathrm{g}+pt_0)^\delta \equiv 1(\mathrm{mod\ p})$.但$\mathrm{g}+pt_0$是模$p$的一个原根，故$(p-1)|\delta$. 另一方面由$\delta$的定义知$\delta|\varphi(p^\alpha)$, 即$\delta|p^{\alpha-1}(p-1)$, 故，$\delta = p^{r-1}\,(p-1)$, 其中$r$是1,2,⋯, α中某一数.

将此结果代人(5)式, 再由(2), (3)及(4)即得

$$1+p^r u_{r-1} \equiv 1(mod\ \ p^\alpha), 即 p^r u_{r-1} \equiv 0(mod\ \ p^\alpha)$$

但$p \nmid u_{r-1}$, 故得$p^r \equiv 0(mod\ \ p^\alpha)$, 由此$\alpha \le r$, 故$r=\alpha$，即$\delta = \varphi(p^\alpha)$.

证完.

定理1.8 （补充） 设$\alpha \geq 1$, g是模p^{α}的一个原根, 则g与$g + p^{\alpha}$中的奇数是模$2p^{\alpha}$的一个原根.

证明： 我们先证明

（Ⅰ）每一奇数x若适合同余式$x^{\gamma} \equiv 1(mod\ p^{\alpha})$及$x^{\gamma} \equiv 1(mod\ 2p^{\alpha})$中的任一个时, 则必适合另一个.

若x适合同余式$x^{\gamma} \equiv 1(mod\ 2p^{\alpha})$, 显然$x$适合同余式$x^{\gamma} \equiv 1(mod\ p^{\alpha})$.

注：补充的定理1.6, 1.7, 1.8，即初等数论（闵嗣鹤，严士健，第四版）定理1, 2, 3，P87-88页

证明： 反之若x适合$x^{\gamma} \equiv 1(mod\ p^{\alpha})$, 由$2 \nmid x$即得$2 \nmid x^{\gamma}$, 因而$x^{\gamma} \equiv 1(mod\ 2)$, 但$(2, p^{\alpha}) = 1$, 故得$x^{\gamma} \equiv 1(mod\ 2p^{\alpha})$.

(II)若g是奇数, 则

$$\mathrm{g}^{\varphi(p^{\alpha})} \equiv 1(mod\ p^{\alpha}), \mathrm{g}^{r} \not\equiv 1(\mathrm{mod}\ p^{\alpha}), 0 < \mathrm{r} < \varphi(p^{\alpha})$$

由(Ⅰ)及$\varphi(p^{\alpha}) = \varphi(2p^{\alpha})$即得

$$\mathrm{g}^{\varphi(2p^{\alpha})} \equiv 1(mod\ 2p^{\alpha}), \mathrm{g}^{r} \not\equiv 1(\mathrm{mod}\ 2p^{\alpha}), 0 < \mathrm{r} < \varphi(2p^{\alpha})$$

故g是模$2p^{\alpha}$的一个原根.

(III)对$\mathrm{g} + p^{\alpha}$是奇数的情形, 其证法与(II)完全相同. 证完.

定理1.6 每个素数 p 均存在模 p 的原根。

证明1 对模 p 的最小非负简化剩余系 $1,2,\cdots,p-1$，按 $\varphi(p)=p-1$ 的因子 d 分类，记 N_d 为其中指数为 d 的元素集合，于是 $\sum_{d|p-1}|N_d|=p-1$。设 $g\in N_d$，则 g 满足同余方程：

$$x^d-1\equiv 0 \bmod p \quad (1.1)$$

即 g 的指数为 d。

由于 $x^d-1\mid x^p-x=x(x^{p-1}-1)$，由第4章定理4.5，方程（1.1）有 d 个解。

由定理1.3的推论2知，在 $1, g, \cdots, g^{d-1}$ 中有 $\varphi(d) = d-1$ 个数指数皆为 d，所以 $g, \cdots, g^{d-1}$ 指数都为 d。即 $\{g, \cdots, g^{d-1}\} \subseteq N_d$，$|N_d| \ldots d-1 = \varphi(d)$。又由第2章定理2.4.1，$\sum_{d|p-1} \varphi(d) = p-1$，所以

$\sum_{d|p-1} (|N_d| - \varphi(d)) = \sum_{d|p-1} |N_d| - \sum_{d|p-1} \varphi(d) = 0$，因此对每个 $d \mid p-1$，有 $|N_d| - \varphi(d) = 0$，所以 $|N_{p-1}| = \varphi(p-1)$。

证毕。

下面讨论 p^{α} 是否有原根，其中 p 为奇素数，$\alpha \ldots 2$ 。为此需要以下2个引理。

引理1 设 p 为奇素数，若 $u \in Z$ 满足 $u^{p-1} = 1 + t_1 p$ ，其中 $t_1 \not\equiv 0 \bmod p$ ，则 $u^{\varphi(p^{\alpha})} = 1 + t_{\alpha} p^{\alpha}$，其中 $t_{\alpha} \not\equiv 0 \bmod p$ 且 $u^{\varphi(p^{\alpha})} \not\equiv 1 \bmod p^{\alpha+1}$。

证明 对 α 用归纳法，$\alpha = 1$ 时，即为 u 满足的条件。设 $\alpha = n$ 时，由 $u^{\varphi(p^n)} = 1 + t_n p^n$ ，其中 $t_n \not\equiv 0 \bmod p$。当 $\alpha = n+1$ 时, 由 $\varphi(p^{n+1}) = p^{n+1} - p^n = p(p^n - p^{n-1}) = p\varphi(p^n)$ 得

$$u^{\varphi(p^{n+1})}=(u^{\varphi(p^n)})^p=(1+t_np^n)^p$$

$$=1+C_p^1(t_np^n)+\sum_{k=2}^{p-1}C_p^k(t_np^n)^k+(t_np^n)^p=1+t_{n+1}p^{n+1}$$，其中

$t_{n+1}=t_n+p(\sum_{k=2}^{p-1}\frac{C_p^k}{p}t_n^kp^{(k-1)n-1}+t_n^pp^{(p-1)n-2})$。由于

$(k-1)n-1\ldots0$，$(p-1)n-2\ldots0$，$p\mid C_p^k$，所以括号内是整数，$t_{n+1}\equiv t_n\not\equiv 0\bmod p$。若 $u^{\varphi(p^\alpha)}\equiv 1\bmod p^{\alpha+1}$，即存在整数 t，使得 $u^{\varphi(p^\alpha)}=1+tp^{\alpha+1}$即 $1+t_\alpha p^\alpha=1+tp^{\alpha+1}$，得 $t_\alpha=tp=0\bmod p$，与 $t_\alpha\not\equiv 0\bmod p$ 矛盾。所以 $u^{\varphi(p^\alpha)}\not\equiv 1\bmod p^{\alpha+1}$。

证毕。

引理2 设 g_0 是模 p 的一个原根，对 $\forall t \in Z$ ，$\alpha \in N$ ，$g_0 + tp$ 模 p^α 的指数 δ 满足：

（1）$\delta \mid \varphi(p^\alpha)$ ；

（2）$(p-1) \mid \delta$ 。

证明 （1） g_0 是模 p 的一个原根，所以 $(g_0, p) = 1$，从而对 $\forall t \in Z$（ $t \neq 0$，否则下面构造的 $g_0 + tp = g_0$ ），$(g_0 + tp, p) = (g_0, p) = 1$，$(g_0 + tp, p^\alpha) = 1$ ，所以 $g_0 + tp$ 在模 p^α 的简化剩余系中。

设 h 是模 p^α 的一个原根。模 p^α 的一个简化剩余系为 $h^0 \equiv 1, h, \cdots, h^{\varphi(p^\alpha)-1}$。设 $g_0 + tp = h^i$，其中 $0 \leq i \leq \varphi(p^\alpha)-1$，则 $\delta = \delta_{p^\alpha}(h^i) = \dfrac{\delta_{p^\alpha}(h)}{(i, \delta_{p^\alpha}(h))} = \dfrac{\varphi(p^\alpha)}{(i, \varphi(p^\alpha))}$，所以 $\delta \mid \varphi(p^\alpha)$。

（2）由 $(g_0 + tp)^\delta \equiv 1 \bmod p^\alpha$，将左边按二项式展开得 $g_0^\delta \equiv 1 \bmod p$，所以 $\varphi(p) = p-1 \mid \delta$。 证毕。

由引理2知，δ是形如 $\varphi(p^m)(1 \leqslant m \leqslant \alpha)$ 的数。还知，要求p^α的原根, 需要在形如 $g_0 + tp$的数中找指数为 $\varphi(p^\alpha)$的数。

定理1.7 设素数 $p>2$，正整数 $\alpha ...2$ ，则模 p^α 必有原根。

证明 由定理1.6知，模 p的原根一定存在，设 g_0为其中一个。由引理1、引理2知，模 p^α 的原根在 $g_0 + tp$的数中找，即求出其中的 t。首先，找 $t_0 \in Z$ $(t_0 \neq 0)$ ，满足

$$(g_0 + t_0 p)^{p-1} = 1 + t_1 p \quad (1.2)$$

其中 $t_1 \not\equiv 0 \bmod p$。由 $g_0^{\varphi(p)} \equiv 1 \bmod p$，可设 $g_0^{p-1} = 1 + lp$ 其中 $l \in Z$。对 $\forall t \in Z$，将 $(g_0 + tp)^{p-1}$ 按二项式展开，展开式中从第3项起都有 p^2 项，得

$$(g_0 + tp)^{p-1} = g_0^{p-1} + C_{p-1}^1 g_0^{p-2} tp + kp^2$$

$$= 1 + p(l + (p-1)g_0^{p-2} t) + kp^2 \qquad (1.3)$$

其中 $k \in Z$。由于 $(p, p-1) = 1$，$(p, g_0^{p-2}) = 1$（g_0^{p-2} 在模 p 的一个简化剩余系中），所以 $(p, (p-1)g_0^{p-2}) = 1$。由 $l + (p-1)g_0^{p-2} t \equiv 0 \bmod p$ 得到的关于 t 的一次同余方程

$$(p-1)g_0^{p-2} t \equiv -l \bmod p \qquad (1.4)$$

有唯一解。

任取 $t_0 \in Z$，使得（1.4）不成立，此时（1.3）式变为

$(g_0 + t_0 p)^{p-1} = 1 + t_1 p$，其中 $t_1 = l + (p-1) g_0^{p-2} t_0 \not\equiv 0 \bmod p$。

由引理2，$g_0 + tp$ 的指数是形如 $\varphi(p^m)(1 \leqslant m \leqslant \alpha)$ 的数。

由引理1，当 $1 \leqslant m < \alpha$ 时，$(g_0 + t_0 p)^{\varphi(p^m)} \not\equiv 1 \bmod p^{m+1}$，

从而 $(g_0 + t_0 p)^{\varphi(p^m)} \not\equiv 1 \bmod p^{\alpha}$。但当 $m = \alpha$ 时，

$(g_0 + t_0 p)^{\varphi(p^{\alpha})} \equiv 1 \bmod p^{\alpha}$。所以 $g_0 + t_0 p$ 就是模 p^{α} 的一个原根。 证毕。

例1.8 求模 11^4 的一个原根。

解 $g_0=2$ 是模11的一个原根，由 $g_0^{p-1}=1+lp$ 得 $2^{10}=1+11\cdot l$, 得 $l=93$。方程(1.4)变为 $10\cdot 2^9 t\equiv -93 \bmod 11$ 任取 $t_0=1$ 使得方程不成立，则 $g_0+t_0 p=2+1\times 11=13$ 就是 11^4 的一个原根。

下面讨论 $2p^{\alpha}(\alpha \ldots 1)$ 的原根。

定理1.8 设素数 $p>2$，g_0 是模 $p^{\alpha}(\alpha\in N)$ 的原根，则 g_0, g_0+p^{α} 中必有一个为奇数，这个奇数就是模 $2p^{\alpha}$ 的一个原根。

证明 由于p^α为奇数，若 g_0为奇数，则 g_0+p^α 为偶数；若 g_0为偶数，则 g_0+p^α 为奇数。即g_0 和 g_0+p^α 中必有一个且仅有一个为奇数, 记这个奇数为 g。$(g,p^\alpha)=(g_0,p^\alpha)=1$ $(g,2)=1$，所以 $(g,2p^\alpha)=1$，g 是模 $2p^\alpha$ 简化剩余系中的元素。

因$1,g_0,g_0^2,\cdots,g_0^{\varphi(p^\alpha)-1}$是模 p^α的一个简化剩余系，$g\equiv g_0 \bmod p^\alpha$ ，所以

$$1,g,g^2,\cdots,g^{\varphi(p^\alpha)-1} \quad (1.5)$$

也是模 p^{α}的一个简化剩余系。（1.5）中元素模 p^{α}两两不同余，模 $2p^{\alpha}$ 也两两不同余，因此是模 $2p^{\alpha}$ 的某个简化剩余系中的元素，因此得 $\varphi(p^{\alpha}) \leqslant \delta_{2p^{\alpha}}(g)$ 。

另一方面，$\delta_{2p^{\alpha}}(g) \leqslant \varphi(2p^{\alpha}) = \varphi(2)\varphi(p^{\alpha}) = \varphi(p^{\alpha})$ 。

所以 $\delta_{2p^{\alpha}}(g) = \varphi(p^{\alpha}) = \varphi(2p^{\alpha})$，即 g 是模 p^{α} 的原根。

证毕。

例1.9 设 $p=3$，求 $2p$ 及 $2p^2$ 的原根。

解 $g_0=2$ 是模3的原根，$\alpha=1$ 时，$g=g_0+p=5$ 为奇数，这个奇数就是模 $2p=6$ 的原根。$\alpha=2$ 时，$g=g_0+p^2=11$ 为奇数，这个奇数就是模 $2p^2=18$ 的原根。

将原根的结论总结一下，得以下定理。

定理1.9 模m存在原根的充要条件是$m=1,2,4,p^{\alpha},2p^{\alpha}$，其中$\alpha\geqslant 1$是整数，$p$是奇素数。

由定理1.8可见，求模$2p^{\alpha}$的原根归结为求p^{α}的原根，由定理1.7可见求p^{α}的原根，需归结为求模p的原根。而求模p的原根只能在模p的简化剩余系中对每个元素验证。

例1.10 设$p=43$，求模p，p^{α}及$2p^{\alpha}(\alpha..1)$的原根。

解 在模43的简化剩余系 $\pm1,\pm2,\cdots,\pm21$ 中逐一验证

$\delta_{43}(1)=1$，$\delta_{43}(2)=14$，而 $3^2\equiv9$ ，$3^3\equiv-16$ ，$3^6\equiv-2$ ，

$3^{14}\equiv-7$ ，$3^{21}\equiv-1$，$3^{42}\equiv1(\mathrm{mod}\,43)$，即 $\delta_{43}(3)=42$ ，

$g_0\equiv3$ 是模43的一个原根。根据定理1.7. 由 $g_0^{p-1}=3^{42}=1+43l$

得 $l=2$。同余方程（1.4）变为 $42\cdot3^{43-2}t\equiv-2\,\mathrm{mod}\,43$，

取 $t_0=1$，使得上述同余方程不成立，$g_0+t_0p=3+1\cdot43=46$

就是 p^α 的一个原根。又因46是偶数，$46+43^\alpha$ 必为奇数，

就是 $2p^\alpha$ 的原根。

6.2 指标与二项同余方程

6.2 指标与二项同余方程

当模m有原根g时，模m的简化剩余系可表示为$g^0=1$，$g^1,\cdots,g^{\varphi(m)-1}$。对$\forall a\in Z$，当$(a,m)=1$时，必可唯一地表示为$a\equiv g^k \bmod m$（$0\leqslant k<\varphi(m)$）。从而当模$m$有原根$g$时，通过$g$，模$m$的简化剩余系与模$\varphi(m)$的完全剩余系之间就建立了一一对应。

定义2.1 设模m有原根g，$(a,m)=1$，如果存在整数$k(0,,\ k<\varphi(m))$，使得$a\equiv g^k \bmod m$，则称k为a对模m以g为底的指标，记作$k=\mathrm{ind}_g a$，简记为$\mathrm{ind}a$。

例2.1　模 $m=11$，$g=2$ 是模11的一个原根，则 $2^0,2^1,\cdots,2^{10-1}$ 是模11的一个简化剩余系。由 $2^0\equiv 1$，$2^1\equiv 2$，$2^2\equiv 4$，$2^3\equiv 8\equiv -3$，$2^4\equiv 5$，$2^5\equiv 10\equiv -1$，$2^6\equiv 9\equiv -2$，$2^7\equiv 7\equiv -4$，$2^8\equiv 3$，$2^9\equiv 6\equiv -5 \pmod{11}$，可得模11的简化剩余系中每个元素对应的指标，列表如下

表6.5 模11以2为底的指标表

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

指标有以下性质：

定理2.1 设 g 是模 m 的原根，$(a,m)=(b,m)=1$，则

（1）$g^{\mathrm{ind}_g a} \equiv a \bmod m$；

（2）$g^h \equiv g^k \bmod m \Leftrightarrow h \equiv k \bmod \varphi(m)$；

（3）$\mathrm{ind}_g(ab) \equiv (\mathrm{ind}_g a + \mathrm{ind}_g b) \bmod \varphi(m)$；

（4）对 $\forall n \in N$，$\mathrm{ind}_g a^n \equiv (n \cdot \mathrm{ind}_g a) \bmod \varphi(m)$；

证明 （1）由定义直接得。

（2）因为 $\delta_m(g)=\varphi(m)$，由定理1.2即得。

（3） 由（1）$a\equiv g^{\mathrm{ind}_g a}$ ，$b\equiv g^{\mathrm{ind}_g b} \bmod m$ ，

$a\cdot b\equiv g^{\mathrm{ind}_g a+\mathrm{ind}_g b} \bmod m$，又 $a\cdot b=g^{\mathrm{ind}_g (ab)} \bmod m$，由(2)

$\mathrm{ind}_g(ab)=(\mathrm{ind}_g a+\mathrm{ind}_g b)\bmod \varphi(m)$。

（4）由（3）即得。

证毕。

由定理2.1可见，$\mathrm{ind}_g a$ 的性质与对数类似。

已知 m, g 时，计算模指数运算 $g^k \bmod m$ 比较容易。但反过来，已知 $a \equiv g^k \bmod m$ 时，计算 $k = \mathrm{ind}_g a$ 则非常困难，称之为离散对数问题，是密码方案常用的数学困难问题之一。

定理2.2 设 g_1 , g_2 是模 m 的2个不同的原根，$(a, m) = 1$，则 $\mathrm{ind}_{g_2} a = (\mathrm{ind}_{g_2} g_1 \cdot \mathrm{ind}_{g_1} a) \bmod \varphi(m)$。

证明 由定理2.1的（1）知 $a \equiv g_1^{\mathrm{ind}_{g_1} a} \bmod m$，

$g_1 \equiv g_2^{\mathrm{ind}_{g_2} g_1} \bmod m$, 所以 $a \equiv (g_2^{\mathrm{ind}_{g_2} g_1})^{\mathrm{ind}_{g_1} a} \equiv g_2^{\mathrm{ind}_{g_2} g_1 \cdot \mathrm{ind}_{g_1} a} \bmod m$

又 $a \equiv g_2^{\mathrm{ind}_{g_2} a} \bmod m$，所以 $g_2^{\mathrm{ind}_{g_2} a} \equiv g_2^{\mathrm{ind}_{g_2} g_1 \cdot \mathrm{ind}_{g_1} a} \bmod m$。

由定理2.1的（2），$\mathrm{ind}_{g_2} a \equiv (\mathrm{ind}_{g_2} g_1 \cdot \mathrm{ind}_{g_1} a) \bmod \varphi(m)$。

证毕。

定理2.2刻画了 a 对模 m 的不同原根的指标之间的关系，相当于对数的换底公式。

下面是指标和指数的关系。

定理2.3 设 g 是模 m 的原根，$(a,m)=1$，则

$$\delta_m(a)=\frac{\varphi(n)}{(\mathrm{ind}_g a,\varphi(n))}$$

证明 设 $a\equiv g^k \bmod m$，则

$$\delta_m(a)=\delta_m(g^k)=\frac{\delta_m(g)}{(k,\delta_m(g))}=\frac{\varphi(m)}{(\mathrm{ind}_g a,\varphi(m))}。$$

证毕。

下面讨论二项同余方程 。

定义2.2 设 $m \geqslant 2$，$(a, m) = 1$，$n \geqslant 2$。如果二项同余方程

$$x^n \equiv a \bmod m \quad (2.1)$$

有解，就称 a 是模 m 的 n 次剩余，否则称为模 m 的 n 次非剩余。

定理2.3 设 $m \geqslant 2$，模 m 有原根 g，$(a, m) = 1$，则二项同余方程 $x^n \equiv a \bmod m$ 有解的充要条件是 $(n, \varphi(m)) \mid \mathrm{ind}_g a$

此外，有解时，有 $(n, \varphi(m))$ 个解。

证明 $x^n \equiv a \bmod m \Leftrightarrow g^{\mathrm{ind}_g x^n} \equiv g^{\mathrm{ind}_g a} \bmod m \Leftrightarrow g^{n\cdot \mathrm{ind}_g x}$

$\equiv g^{\mathrm{ind}_g a} \bmod m \Leftrightarrow n\cdot \mathrm{ind}_g x \equiv \mathrm{ind}_g a \bmod \varphi(m)$，其中第1步由定理2.1的（1）得，第2步由定理2.1的（4）、第3步由定理2.1的（2）得。

设 $y = \mathrm{ind}_g x$ ，因此求二项同余方程 $x^n \equiv a \bmod m$ 等价于求一次同余方程 $n\cdot y \equiv \mathrm{ind}_g a \bmod \varphi(m)$ ，由第4章定理2.1，该方程有解的充要条件是 $(n,\varphi(m)) \mid \mathrm{ind}_g a$ ，而且它的解数为 $(n,\varphi(m))$。求出 y后。可得 $x \equiv g^y \bmod m$ 。

证毕。

例2.2 求解同余方程 $x^8 \equiv 5 \bmod 11$ 。

解 已知 $g=2$ 是模11的一个原根，由表6.5知 $\mathrm{ind}_2 5 = 4$ ，所以方程等价于 $8y \equiv 4 \bmod 10$ 。$(8,10)=2|4$ ，所以有2个解，$y \equiv 3,8 \pmod{10}$ 。再由表6.5知指标3、8对应的元素为 $\pm 3 \bmod 11$ ，即为原方程的解。

例2.3 求解同余方程 $6\cdot 8^x \equiv 9 \bmod 13$ 。

解 容易验证 2是模13的一个原根，构造指标表如下。

表6.6 模13以2为底的指标表

a	-6	-5	-4	-3	-2	-1	1	2	3	4	5	6
$\mathrm{ind}_2 a$	11	3	8	10	7	6	0	1	4	2	9	5

同余方程等价于 $\mathrm{ind}_2 6 + x\cdot \mathrm{ind}_2 8 \equiv \mathrm{ind}_2 9 \bmod 12$ ，即 $5+3x \equiv 8 \bmod 12$ ，$3x \equiv 3 \bmod 12$ ，$x \equiv 1 \bmod 4$ ，所以方程的解为1，5，9（mod12）。

习题

1. 设 p 为素数，$\delta_p(a)=3$，证明：

（1）$\sum_{k=0}^{3} a^k \equiv 1 \bmod p$ ；（2）$\delta_p(1+a)=6$ 。

2. 设 $(a,2)=1$ ，$l \geq 3$, 用数学归纳法证明 $a^{2^{l-2}} \equiv 1 \bmod 2^l$

3. 设 n 为正整数，$(a,n)=(b,n)=1$，证明：

（1）$\delta_n(ab)=\delta_n(a)\delta_n(b) \Leftrightarrow (\delta_n(a),\delta_n(b))=1$ ；

（2）存在 c，使得 $\delta_n(c)=[\delta_n(a),\delta_n(b)]$。

4. 设 p 为奇素数，g 为模 p 的原根，

（1）证明：$g^2, g^4, \cdots, g^{p-1}$ 为模 p 的二次剩余；$g, g^3, \cdots, g^{p-2}$ 为模 p 的二次非剩余；

（2）利用（1）证明 $g^{\frac{p-1}{2}} \equiv -1 \bmod p$ 。

5. 设 p 为奇素数，a, b 为模 p 的2个原根，证明：$\delta_p(ab) < \varphi(p)$

6. 设 p 为素数，

（1）若 $p \equiv 1 \bmod 4$ ，g 为模 p 的原根，证明：$-g$ 也是模 p 的原根；

（2）若 $p \equiv 3 \bmod 4$，证明：g 为模 p 的原根 $\Leftrightarrow \delta_p(-g) = \dfrac{p-1}{2}$

7. （1）求模23的一个原根，并由原根构造模23的指数表；

（2）求解同余方程 $x^8 \equiv 41 \bmod 23$ 。

8. （1）求所有整数 m，使得关于 x 的同余方程

$mx^5 \equiv 7 \bmod 29$ 有解；

（2）求所有整数 n 使得同余方程 $5x^6 \equiv n \bmod 23$ 有解且 $23 \nmid n$。