第 4 章 指数与原根

在一个模 m 的既约剩余系中，如果一个元素的指数恰好等于 $\phi(m)$，则这个元素即为模 m 的一个原根．在存在原根的既约剩余系中，每个元素均可以表示成原根的幂，反过来原根的幂所表示的所有不同的元素恰好构成既约剩余系，这就给出了一种构造模 m 的既约剩余系的很自然的一种方法．但只有 $m=1, 2, 4, p^{\alpha}, 2p^{\alpha}$ 时才有原根，对于不存在原根的模 m，它的既约剩余系是怎样构造的呢？以上所描述的结论与问题正是本章所要研究的主要内容．另外，本章还介绍指数、指标两个主要概念及性质，其中指标为密码学中的离散对数问题．离散对数问题是设计许多公钥密码算法的重要理论根据．

§1 指数及其性质

首先我们给出指数及其原根的概念．

定义 1 设 $m \ge 1$，$(a, m)=1$． 使式

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

成立的最小的正整数 d 称为 a **对模 m 的指数**（习惯上也称为**阶或周期**），记作 $\delta_m(a)$．当 $\delta_m(a)=\phi(m)$ 时，称 a 是**模 m 的原根**．

性质 1 设 $m \ge 1$，$(a, m)=1$．对任意整数 d，如果

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

则 $\delta_m(a) \mid d$．

证明 设 $d_0=\delta_m(a)$，则 $d=qd_0+r$，$0 \le r < d_0$

$$a^{d}-1=a^{qd_0+r}-1=(a^{d_0})^{q}a^{r}-1 \equiv a^{r}-1 \equiv 0 (\bmod m)$$

因为 $0 \le r < d_0$，所以由指数的定义得 $r=0$．得证．

指数还具有以下特性：

性质 2 若 $b \equiv a(\bmod m)$，$(a,m)=1$，则 $\delta_m(a)=\delta_m(b)$.

性质 3 $\delta_m(a) \mid \phi(m)$；$\delta_{2^l}(a) \mid 2^{l-2}$，$l \geq 3$.

利用性质 3 可验证下列例子的正确性.

例 1 列出模 $m=17$ 的既约剩系的所有元素的指数.

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\delta(a)$	1	8	16	4	16	16	16	8	8	16	16	16	4	16	8	2

由 $\phi(m)=16$ 及表知模 17 的原根为 $3,5,6,7,10,11,12,14(\bmod 17)$.

例 2 列出模 $m=2^5$ 的既约剩系的所有元素的指数.

a	1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31
$\delta(a)$	1	8	8	4	4	8	8	2	2	8	8	4	4	8	8	2

由 $\phi(m)=2^4=16$ 及表知模 $m=2^5$ 无原根.

性质 4 若 $(a,m)=1$，

$$a^i \equiv a^j (\bmod m),$$

则

$$i \equiv j(\bmod \delta_m(a)).$$

性质 5 设

$$aa^{-1} \equiv 1(\bmod m),$$

则

$$\delta_m(a)=\delta_m(a^{-1}).$$

性质 2、3、4、5 的证明非常简单，留作练习.

性质 6 设 k 是非负整数，则有

$$\delta_m(a^k)=\frac{\delta_m(a)}{(\delta_m(a), \quad k)}.$$

而且，在模 m 的一个既约剩余系中，至少有 $\phi(\delta_m(a))$ 个数对模 m 的指数等于 $\delta_m(a)$.

证明 记

$$\delta=\delta_m(a),\quad \delta'=\delta/(\delta,k),\quad \delta''=\delta_m(a^k).$$

先证明$\delta'|\delta''$，由题意得

$$a^{\delta}\equiv 1(\bmod m)，\ (a^k)^{\delta''}\equiv 1(\bmod m).$$

由性质 1 得$\delta|k\delta''$，所以

$$\delta'=\frac{\delta}{(\delta,k)}\Big|\frac{k\delta''}{(\delta,k)},$$

因为

$$(\frac{\delta}{(\delta,k)},\frac{k}{(\delta,k)})=1,$$

故$\delta'|\delta''$.

再证明$\delta''|\delta'$，由

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

知，$\delta''|\delta'$成立．所以$\delta'=\delta''$，得证.

由性质 6 可以的到以下两个重要推论.

推论 1 当$(k,\delta_m(a))=1$时，$\delta_m(a)=\delta_m(a^k)$.

推论 1 是一个很重要的结论，它不仅可以确定原根及原根的个数，而且可以用于确定有限循环限群的生成元及生成元的个数．从而有

推论 2 若g为模m的原根，则模m的原根的个数为$\phi(\phi(m))$，并且

$$\{g^i\,|\,(i,\phi(m))=1,\quad 1\le i<\phi(m)\}$$

即为所有原根的集合.

性质 7 $\delta_m(ab)=\delta_m(a)\delta_m(b)$的充要条件是$(\delta_m(a),\delta_m(b))=1$.

证明 设

$$\delta=\delta_m(ab)，\ \delta'=\delta_m(a)，\ \delta''=\delta_m(b)，\ \eta=[\delta_m(a),\delta_m(b)].$$

充分性：首先

$$1\equiv (ab)^{\delta}\equiv (ab)^{\delta\delta''}\equiv a^{\delta\delta''}(\bmod m),$$

所以，$\delta'\big|\delta\delta''$．又因为$(\delta',\delta'')=1$，故$\delta'\big|\delta$．同理，

$$1\equiv(ab)^{\delta}\equiv(ab)^{\delta\delta'}\equiv b^{\delta\delta'}(\bmod m),$$

所以，$\delta''\big|\delta\delta'$ ，从而$\delta''\big|\delta$．又因为$(\delta',\delta'')=1$，故$\delta'\delta''\big|\delta$．另一方面显然

$$(ab)^{\delta'\delta''}\equiv 1(\bmod m),$$

故$\delta\big|\delta'\delta''$，因此$\delta=\delta'\delta''$．

必要性：我们有$(ab)^{\eta}\equiv 1(\bmod m)$，所以$\delta\big|\eta$，由$\delta=\delta'\delta''$得$\delta'\delta''\big|\eta$，另外显然，$\eta\big|\delta'\delta''$．

故$\delta'\delta''=\eta$，即$(\delta',\delta'')=1$．

性质 8 （1）若$n\big|m$，则$\delta_n(a)\big|\delta_m(a)$；

（2）若$(m_1,m_2)=1$，则

$$\delta_{m_1m_2}(a)=[\delta_{m_1}(a),\delta_{m_2}(a)].$$

证明 （1）由

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

知

$$a^{\delta_m(a)}\equiv 1(\bmod n),$$

从而知$\delta_n(a)\big|\delta_m(a)$，（1）得证.

（2） 记$\delta'=[\delta_{m_1}(a),\delta_{m2}(a)]$，由于

$$\delta_{m_1}(a)\,|\,\delta_{m_1,m_2}(a),\quad \delta_{m_2}\,|\,\delta_{m_1,m_2}(a),$$

所以$\delta'\,|\,\delta_{m_1,m_2}(a)$．　另一方面，

$$a^{\delta'}\equiv 1(\bmod m_j),(j=1,2),$$

又因为$(m_1,m_2)=1$推出

$$a^{\delta'}\equiv 1(\bmod m_1m_2),$$

因而$\delta_{m_1,m_2}(a)\mid\delta'$，$\delta_{m_1,m_2}(a)=\delta'$.

由性质 8 可以推出更一般的性质（即性质 9）成立.

性质 9 若$m=2^{\alpha_0}p_1^{\alpha_1}\cdots p_s^{\alpha_s}$，$p_i$是两两不同的奇素数，则$\delta_m(a)\mid\lambda(m)$，其中

$$\lambda(m)=[2^{c_0},\phi(p_1^{\alpha_1}),\cdots,\phi(p_s^{\alpha_s})]，\quad c_0=\begin{cases}0, & \alpha=0,1;\\ 1, & \alpha=2;\\ \alpha-2, & \alpha\ge 3.\end{cases}$$

$\lambda(m)$称为 Carmichael 函数.

性质 10 设$(m_1,m_2)=1$. 那么对任意a_1,a_2，必有a使得

$$\delta_{m_1m_2}(a)=[\delta_{m_1}(a_1),\delta_{m_2}(a_2)].$$

证明 考虑同余方程组

$$x\equiv a_1(\operatorname{mod} m_1),\quad x\equiv a_2(\operatorname{mod} m_2),$$

由孙子定理知，同余方程组有唯一解

$$x\equiv a(\operatorname{mod} m_1m_2).$$

显然有

$$\delta_{m_1}(a)=\delta_{m_1}(a_1),\quad \delta_{m_2}(a)=\delta_{m_2}(a_2).$$

由此从性质8就推出所要结论.

性质 11 对任意a, b，一定存在c，使

$$\delta_m(c)=[\delta_m(a),\delta_m(b)].$$

证明 设$\delta'=\delta_m(a)$，$\delta''=\delta_m(b)$，$\eta=[\delta',\delta'']$. 则可对δ',δ''作如下分解

$$\delta'=\tau'\eta'，\quad \delta''=\tau''\eta'',$$

其中

$$(\eta',\eta'')=1，\quad \eta'\eta''=\eta.$$

由性质 6 可得

$$\delta_m(a^{\tau'})=\eta'，\quad \delta_m(b^{\tau''})=\eta''.$$

再由性质 7 得

$$\delta_m(a^{\tau'}b^{\tau''})=\delta_m(a^{\tau'})\delta_m(b^{\tau''})=\eta'\eta''=\eta .$$

从而，取 $c=a^{\tau'}b^{\tau''}$ 即可.

例 3 设 $m>1$，$(ab,m)=1$，再设 λ 是使

$$a^d\equiv b^d(\bmod m)$$

成立的最小的正整数．证明：

（1）若 $a^k\equiv b^k(\bmod m)$ 成立，则 $\lambda\mid k$；

（2）$\lambda\mid\phi(m)$.

证明（1）设 $k=\lambda q+r$，$0\le r<\lambda$.

$$a^k=a^{\lambda q+r}=a^{\lambda q}a^r\equiv b^k=b^{\lambda q+r}=b^{\lambda q}b^r(\bmod m),$$

因为

$$a^{\lambda}\equiv b^{\lambda}(\bmod m),\ (ab,m)=1,$$

所以根据同余的性质得

$$a^r\equiv b^r(\bmod m).$$

由于 λ 为使上式成立的最小的正整数，从而 $r=0$，即 $\lambda\mid k$.

（2）由于 $(ab,m)=1$，由 Euler 定理

$$a^{\phi(m)}\equiv 1\equiv b^{\phi(m)}(\bmod m),$$

由（1）得 $\lambda\mid\phi(m)$.

§2 原根及其性质

下面定理说明了模 m 有原根的充要条件.

定理 1 模 m 有原根的充要条件是 $m=1,\ 2,\ 4,\ p^{\alpha},\ 2p^{\alpha}$，其中 p 是奇素数，$\alpha\ge 1$.

定理的必要性证明　当m不属于上述情况时，必有

$$m=2^{\alpha}\ (\alpha\geq 3)\text{，}\ m=2^{\alpha}p_1^{\alpha_1}\cdots p_r^{\alpha_r}\ (\alpha\geq 2,r\geq 1)\text{，}$$

或

$$m=2^{\alpha}p_1^{\alpha_1}\cdots p_r^{\alpha_r}(\alpha\geq 0,r\geq 2)\text{，}$$

其中p_i为不同的奇素数，$a_i\geq 1(1\leq i\leq r)$.

设

$$\lambda(m)=[2^{c_0},\phi(p_1^{\alpha_1}),\cdots,\phi(p_r^{\alpha_r})]\text{，}\ c_0=\begin{cases}0, & \alpha=0,1;\\ 1, & \alpha=2;\\ \alpha-2, & \alpha\geq 3.\end{cases}$$

容易验证，当m属于假设的三种情况任意一种时，都有$\lambda(m)<\phi(m)$，由上一节性质知$\delta_m(a)\,|\,\lambda(m)$，因此$\delta_m(a)<\phi(m)$，此时模没有原根.

在证明定理的充分性之前首先证明两个引理.

引理 1 设p是素数，则模p必有原根.

证明 由指数的性质知，一定存在整数g使得

$$\delta_p(g)=[\delta_p(1),\delta_p(2),\cdots,\delta_p(p-1)]=\delta\ .$$

下证$\delta=p-1$. 显然$\delta\,|\,p-1$，从而$\delta\leq p-1$. 由于$\delta_p(i)\,|\,\delta,\quad i=1,2,\cdots,p-1$. 因而同余方程

$$x^{\delta}\equiv 1(\operatorname{mod} p)$$

有解$x=1,2,\cdots,p-1(\operatorname{mod} p)$. 又因为同余方程解的个数$n\leq\min\{\delta,p\}$，所以$p-1\leq\delta$. 故可得到$\delta=p-1$，这就说明了$g$是模$p$的原根.

引理 2 设p是奇素数，那么对任意的$a\geq 1$，模p^{α}，$2p^{\alpha}$均有原根.

证明　分如下五步证明该定理.

1)　若g是模$p^{\alpha+1}(\alpha\geq 1)$的原根，　则$g$一定是模$p^{\alpha}$的原根只需证明$\delta_{p^{\alpha}}(g)=\phi(p^{\alpha})$.

设$\delta=\delta_{p^{\alpha}}(g)$，可得$\delta\,|\,\phi(p^{\alpha})$. 由

$$g^{\delta}\equiv 1(\operatorname{mod} p^{\alpha})$$

可推出

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

由 g 是模 $p^{\alpha+1}$ 的原根知

$$\phi(p^{\alpha+1}) = \delta_{p^{\alpha+1}}(g) \mid p\delta .$$

又因为

$$\phi(p^{\alpha+1}) = p^{\alpha}(p-1) ,$$

所以 $\phi(p^{\alpha}) \mid \delta$. 从而 $\delta = \phi(p^{\alpha})$，即 g 一定是模 p^{α} 的原根.

2) 若 g 是模 p^{α} 的原根，则必有 $\delta_{p^{\alpha+1}}(g) = \phi(p^{\alpha})$ 或 $\phi(p^{\alpha+1})$.

因为 $p^{\alpha} \mid p^{\alpha+1}$，由上一节性质 8 知

$$\phi(p^{\alpha}) = \delta_{p^{\alpha}}(g) \mid \delta_{p^{\alpha+1}}(g) ,$$

又因为 $\delta_{p^{\alpha+1}}(g) \mid \phi(p^{\alpha+1})$，所以

$$\delta_{p^{\alpha+1}}(g) = \phi(p^{\alpha}) \text{ 或 } \phi(p^{\alpha+1}) .$$

3) 当 p 是奇素数时，若 g 是模 p 的原根，且有

$$g^{p-1} = 1 + rp，\ (p, r) = 1 ,$$

则 g 是模 $p^{\alpha} (\alpha \geq 1)$ 的原根.

用归纳法证明对 $\alpha \geq 1$ 有

$$g^{\phi(p^{\alpha})} = 1 + r(\alpha) p^{\alpha}，\ (p, r(\alpha)) = 1 .$$

当 $\alpha = 1$ 时显然成立. 假设对 $\alpha = n (n \geq 1)$ 成立. 当 $\alpha = n+1$ 时,

$$\begin{aligned} g^{\phi(p^{n+1})} &= (1 + r(n) p^{n})^{p} \\ &= 1 + r(n) p^{n+1} + \frac{1}{2} p(p-1) r^{2}(n) p^{2n} + \cdots = 1 + r(n+1) p^{n+1} . \end{aligned}$$

由于 $(p, r(n)) = 1$，所以 $(p, r(n+1)) = 1$，即对 $\alpha = n+1$ 也成立.

由于对 $\alpha \geq 1$ 有

$$g^{\phi(p^\alpha)} = 1 + r(\alpha)p^\alpha\text{，}\ (p, r(a)) = 1$$

成立，以及⑵就推出 g 是模 $p^\alpha(\alpha \ge 1)$ 的原根．

4)　当 p 是奇素数时，g' 是模 p 的原根且为奇数（若 g' 是偶数则以 $g'+p$ 代替）．那么

$$g = g' + tp\text{，}\ t = 0, 1, \cdots, p-1$$

都是模 p 的原根，且除了一个以外，都满足

$$g^{p-1} = 1 + rp\text{，}\ (p, r) = 1.$$

因为

$$g^{p-1} = (g'+tp)^{p-1} = (g')^{p-1} + (p-1)(g')^{p-2}pt + Ap^2\text{，}$$

其中 A 为整数，设 $(g')^{p-1} = 1 + ap$，由上式得

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

又由于 $(p,\ (p-1)g') = 1$，所以 t 的一次同余方程

$$(p-1)(g')^{p-2}t + a \equiv 0 \pmod p$$

的解数为 1．这就证明了所要结论．由于 $t = 0, 1, \cdots, p-1$ 中至少有两个偶数及 g' 本身．所以总可取到模 p 的原根为奇数且满足 $g^{p-1} = 1 + rp$，$(p, r) = 1$，我们把它记作 $\overline{g}$．

5)　由⑶和⑷立即推出 $\overline{g}$ 是所有模 $p^\alpha(\alpha \ge 1)$ 的原根，由于 $\overline{g}$ 为奇数，所以

$$(\overline{g})^d \equiv 1 \pmod{p^\alpha}$$

与

$$(\overline{g})^d \equiv 1 \pmod{2p^\alpha}$$

等价．因此

$$\delta_{2p^\alpha}(\overline{g}) = \delta_{p^\alpha}(\overline{g}) = \phi(p^\alpha)\text{，}$$

由此及 $\phi(2p^\alpha) = \phi(p^\alpha)$ 就推出 $\overline{g}$ 是所有模 $2p^\alpha(\alpha \ge 1)$ 的原根．

事实上，存在 $\overline{g}$ 使得对所有的 $a \ge 1$，$\overline{g}$ 是模 p^α，模 $2p^\alpha$ 的公共原根．

定理的充分性证明

由引理 1 与引理 2 知，当 $m = p,\ p^{\alpha}, 2p^{\alpha}$ 时，模 m 有原根．对任意的 $a \geq 1$，模 p^{α} 必有原根．事实上，存在 $\overline{g}$ 使得对所有的 $a \geq 1$，$\overline{g}$ 是模 p^{α}，模 $2p^{\alpha}$ 的公共原根．当 $m = 1, 2, 4$ 时，易证原根分别为 $1, 1, -1$．所以当 $m = 1, 2, 4,\ p^{\alpha}, 2p^{\alpha}$（$p$ 是奇素数）时，模 m 有原根．定理得证．

根据定理 1 知，对于寻找模 $m = p$ 的原根，方法比较复杂，因为一般需要分解 $\phi(m)$ 的因子，并且根据原根的定义还需要对 $\phi(m)$ 所有除数 $d < \phi(m)$，验证 $a^d \not\equiv 1(\bmod m)$．因此具体求原根问题确是一个困难问题，也没有一般的方法．下面定理 2 提供了在已知 m 的分解因子的情况下寻找原根的一种较简单的方法，这也是密码学最为常用的寻找原根的方法．

定理 2 设 $m = 1, 2, 4, p^{\alpha}, 2p^{\alpha}$（$p$ 是奇素数），$\phi(m)$ 的所有不同的素因子为 $q_1, q_2, \ldots q_s$．那么 g 是模 m 的原根的充要条件是

$$g^{\phi(m)/q_j} \not\equiv 1(\bmod m), \quad j = 1, \cdots, s.$$

对于每个随机选取的随机数 a 根据定理 2 可以检测 a 是否为原根．由上节推论 2 知原根分布的平均概率为 $\phi(\phi(m))/m$，这个概率表明用随机的方法可以在多项式时间内找到的一个原根．引理 2 与定理 2 提供了密码学中寻找原根的常用的概率方法．

例 1 求模 $p = 47$ 的原根．

解 $p = 47$，$\phi(p) = 46 = 2 \times 23$；

$a = 2$ 时，

$$2^{46/23} = 4 \not\equiv 1(\bmod 47),\quad 2^{46/2} = 2^{23} \equiv 1(\bmod 47),$$

所以 2 不是 47 的原根．

$a = 3$ 时，

$$3^{46/23} = 9 \not\equiv 1(\bmod 47),\quad 3^{46/2} = 3^{23} \equiv 1(\bmod 47),$$

所以 3 不是 47 的原根．

$a = 4$ 时，

$$4^{46/23} = 16 \not\equiv 1(\bmod 47),\quad 4^{46/2} = 4^{23} \equiv 1(\bmod 47),$$

所以 4 不是 47 的原根．

$a=5$时，

$$5^{46/23}=25\not\equiv 1(\mathrm{mod}\,47)，\ 5^{46/2}=5^{23}\neq 1(\mathrm{mod}\,47)，$$

所以 5 是 47 的原根.

例 2 求模 $p=61$的原根.

解 $p=61$，$\phi(p)=60=2^2\times 3\times 5$.

$a=2$时，

$$2^{60/5}=2^{12}\not\equiv 1(\mathrm{mod}\,47)，\ 2^{60/3}=2^{20}\not\equiv 1(\mathrm{mod}\,47)，\ 2^{60/2}=2^{30}\not\equiv 1(\mathrm{mod}\,47)，$$

所以 2 为 61 的原根.

§3 指标、既约剩余系的构造

指标是初等数论中一个基本的概念，求指标问题即为密码学中经常提到的求离散对数问题. 在密码学中，在表示上习惯用指标的英文形式$index_{m,g}(a)$，但习惯上称为离散对数（Discrete logarithm）.

定理 1 如果模 m 存在原根，则任一原根 g 可以生成模 m 的既约剩余系，即$\{g^0,g^1,...,g^{\phi(m)-1}\}$构成模$m$的既约剩余系.

证明 由原根的定义知使$\phi(m)$就是使

$$g^d\equiv 1(\mathrm{mod}\,m)$$

成立的最小的正整数，从而易证当$i\neq j$时，

$$g^i\not\equiv g^j(\mathrm{mod}\,m),\quad 0\le i<\phi(m),\quad 0\le j<\phi(m).$$

定理得证.

通常称原根g为模m的简化剩余系的一个生成元，这与有限循环群的生成元是一致的.

定义 1 g为模m的原根，给定a，$(a,m)=1$，则存在唯一的$\gamma, 0\le\gamma<\phi(m)$，使得

$$a\equiv g^{\gamma}(\mathrm{mod}\,m),$$

我们把γ称为是a**对模**m**的以**g**为底的指标（或离散对数）**. 记为$\gamma_{m,g}(a)$（或$index_{m,g}(a)$），

当模 m 与原根 g 很明确时，也可以简记为 $\gamma_g(a)$、$\gamma(a)$（或 $index_g(a)$、$index(a)$）.

下面定理说明了模 $m=2^{\alpha},\alpha\ge 3$ 的既约剩余系中，一定存在一个元素 g_0 满足 $\delta_{2^{\alpha}}(g_0)=2^{\alpha-2}$．更具体的说，$g_0$ 可以取值为 5.

定理 2 设 $m=2^{l}\ (l\ge 3)$，$a=5$．证明：使

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

成立的最小的正整数 d_0 为 2^{l-2}.

证明 由 $\phi(2^l)=2^{l-1}$，及 $d_0\mid\phi(2^l)$ 知 $d_0=2^k$，$0\le k\le l-1$.

（1）先证对任意的 a，$2\nmid a$ 必有

$$a^{2^{l-2}}\equiv 1(\bmod 2^{l}). \qquad (1)$$

对 l 用归纳法来证．设 $a=2t+1$．当 $l=3$ 时，

$$a^{2}=4t(t+1)+1\equiv 1(\bmod 2^{3}),$$

所以（1）式成立．假设当 $l=n(n\ge 3)$ 时，（1）式成立．当 $l=n+1$ 时，由

$$a^{2^{n-1}}-1=(a^{2^{n-2}}-1)(a^{2^{n-2}}+1)$$

及假设得

$$a^{2^{n-1}}\equiv 1(\bmod 2^{n+1}),$$

即对 $l=n+1$ 式（1）成立.

（2）下面来证 $a=5$ 时，对任意的 $l\ge 3$，必有

$$5^{2^{l-3}}\not\equiv 1(\bmod 2^{l}).$$

当 $l=3$ 时可直接验证成立．假设 $l=n(l\ge 3)$，结论成立．当 $l=n+1$ 时，由（1）的结论知

$$5^{2^{l-3}}\equiv 1(\bmod 2^{l-1}),\quad l\ge 3,$$

因而

$$5^{2^{n-3}}=1+s\cdot 2^{n-1},\quad 2\nmid s.$$

从而

$$5^{2^{n-2}}=1+s(1+s\cdot 2^{n-2})2^n，\quad 2\nmid s(1+s\cdot 2^{n-2})$$

故当 $l=n+1$ 时，结论也成立.

由以上两部分知 $a=5$，使 $a^d\equiv 1(\bmod m)$ 成立的最小的正整数 d_0 为 2^{l-2} .

定义 2 在模 $m=2^\alpha,\alpha\geq 3$ 的既约剩余系中，如果存在一个元素 g_0 满足 $\delta_{2^\alpha}(g_0)=2^{\alpha-2}$ 时，则

$$\pm {g_0}^0,\pm {g_0}^1,\cdots,\pm {g_0}^{2^{\alpha-2}-1}$$

为模 $m=2^\alpha,\alpha\geq 3$ 的一个既约剩余系．那么，任给 $a,(a,2)=1$，a 可唯一表示为

$$a\equiv(-1)^{\gamma^{(-1)}}g_0^{\gamma^{(0)}}(\bmod 2^\alpha)，\quad 0\leq\gamma^{(-1)}<2，\quad 0\leq\gamma^{(0)}<2^{\alpha-2}.$$

我们把 $\gamma^{(-1)},\gamma^{(0)}$ 称为是 a 对模 2^α 的以 $-1,\ g_0$ 为底的指标组．记为 $\gamma^{(-1)}_{2^\alpha;-1,g_0}(a)$，$\gamma^{(0)}_{2^\alpha;0,g_0}(a)$，或简记为 $\gamma^{(-1)}(a),\gamma^{(0)}(a)$ 或 $\gamma^{(-1)}_{g_0}(a),\gamma^{(0)}_{g_0}(a)$.

关于模 2^α 的以 $-1,\ g_0$ 为底的指标组 $\gamma^{(-1)}_{2^\alpha;-1,g_0}(a)$，$\gamma^{(0)}_{2^\alpha;0,g_0}(a)$，我们只讨论 $g_0=5$ 的情况，且简记为 $\gamma^{(-1)}(a),\gamma^{(0)}(a)$.

下面先讨论一下指标与指标组的性质.

定理 3 设 g 是模 m 的原根，$(a,m)=1$．则

$$g^h\equiv a(\bmod m)$$

的充要条件是

$$h\equiv\gamma_{m,g}(a)(\bmod\phi(m)).$$

定理 4 设 g 是模 m 的原根，$(ab,m)=1,$ 则有

$$\gamma_{m,g}(ab)\equiv\gamma_{m,g}(a)+\gamma_{m,g}(b)(\bmod\phi(m)).$$

定理 5 设 $g,\ g'$ 模 m 的两个不同的原根，$(a,m)=1$，我们有

$$\gamma_{m,g'}(a)\equiv\gamma_{m,g'}(g)\gamma_{m,g}(a)(\bmod\phi(m)).$$

这个定理相当于对数的换底公式. 以上这三个定理的证明非常简单，留给读者自己证明. 再

看几关于指数与指标关系的个定理.

定理 6　设 g 是模 m 的原根，$(a,m)=1$．则

$$\delta_m(a)=\frac{\phi(m)}{(\gamma_{m,g}(a),\phi(m))}.$$

由此推出，当模 m 有原根时，对每个正除数 $d|\phi(m)$，在模 m 的一个既约剩余系中，恰有 $\phi(d)$ 个元素对模 m 的指数等于 d，特别地，恰有 $\phi(\phi(m))$ 个原根.

证明　由在指数的性质知

$$\delta_m(a^k)=\delta_m(a)/(k,\delta_m(a)).$$

令 $a=g$，$k=\gamma_{m,g}(a)$，因为 $\delta_m(g)=\phi(m)$，则

$$\delta_m(a)=\phi(m)/(\gamma_{m,g}(a),\phi(m))$$

成立．g 是模 m 的原根，所以模 m 的既约剩余系可表为

$$g^0=1,g^1,\cdots g^{\phi(m)-1}$$

的形式，其中元素 g^i 的指数 $\delta_m(g^i)=d$ 的充要条件是

$$(\phi(m),i)=\phi(m)/d,\quad 0\le i<m.$$

设 $i=t\times\phi(m)/d$，上式等价于 $(d,t)=1, 0\le t<d$，满足上式的 t 恰有 $\phi(d)$ 个．定理得证.

由定理 6 的证明知 $\phi(\phi(m))$ 个原根分别是 $g^t, 0\le t<\phi(m)$，$(t,\phi(m))=1$.

我们通过计算 $g^i,1\le i\le\phi(m)$ 的绝对最小剩余，把这些结果按指标大小或既约剩余系的大小列表，叫做**指标表.**

例 1　构造模 17 以 3 为原根的指标表.

$\gamma_{17,3}(a)$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6
$\delta(a)$	1	16	8	16	4	16	8	16	2	16	8	16	4	16	8	16

表 1

定理 7　给定模 2^α，若

$$a \equiv (-1)^j 5^h (\bmod 2^\alpha),$$

则有

$$j \equiv \gamma^{(-1)}(a) \equiv {(a-1)}/{2} (\bmod 2)$$

及

$$h \equiv \gamma^{(0)}(a) (\bmod 2^{\alpha-2}).$$

定理 8　给定模 2^α，　设 $(ab, 2) = 1$，则

$$\gamma^{(-1)}(ab) \equiv \gamma^{(-1)}(a) + \gamma^{(-1)}(b) (\bmod 2)$$

及

$$\gamma^{(0)}(ab) \equiv \gamma^{(0)}(a) + \gamma^{(0)}(b) (\bmod 2^{\alpha-2}).$$

这两个定理的证明较简单，我们留作习题.

定理 9 设 $(a, 2) = 1$，则

$$\delta_{2^\alpha}(a) = \begin{cases} 2^{\alpha-2} / (\gamma^{(0)}(a), 2^{\alpha-2}), & 0 < \gamma^{(0)}(a) < 2^{\alpha-2}; \\ 2 / (\gamma^{(-1)}(a), 2), & \gamma^{(0)}(a) = 0. \end{cases}$$

证明　$\gamma^{(0)} = 0$ 的充要条件是

$$a \equiv (-1)^{\gamma^{(-1)}(a)} \equiv \pm 1 (\bmod 2^\alpha),$$

容易验证此时上式成立.

当 $0 < \gamma^{(0)}(a) < 2^{\alpha-2}$ 时，一定有

$$a \not\equiv 1 (\bmod 2^\alpha),$$

所以 $2 \mid \delta_{2^\alpha}(a)$． 设 $b = 5^{\gamma^{(0)}(a)}$，记 $\delta(a) = \delta_{2^\alpha}(a), \delta(b) = \delta_{2^\alpha}(b)$，由指标的性质知

$$\delta(b) = 2^{\alpha-2} / (\gamma^{(0)}(a), 2^{\alpha-2}).$$

由 $0 < \gamma^{(0)}(a) < 2^{\alpha-2}$　知　$2 \mid \delta(b)$．由 $2 \mid \delta(a)$ 推出

$$1 \equiv a^{\delta(a)} \equiv ((-1)^{\gamma^{(-1)}(a)} b)^{\delta(a)} \equiv b^{\delta(a)} (\bmod 2^\alpha).$$

由 $2\left|\delta(b)\right.$ 推出

$$a^{\delta(b)} \equiv \left((-1)^{\gamma^{(-1)}(a)}b\right)^{\delta(b)} \equiv b^{\delta(b)} \equiv 1\left(\bmod 2^{\alpha}\right).$$

从而得　$\delta(a)\left|\delta(b)\right.$ 及 $\delta(b)\left|\delta(a)\right.$．故 $\delta(a)=\delta(b)$ 进而结论成立．

当 $d>2, d\left|2^{\alpha-2}\right.$ 时，可设 $d=2^{j}, 1<j\le 2^{\alpha-2}$．由上面定理，

$$\delta_{2^{\alpha}}(a)=d=2^{j}$$

的充要条件是

$$(\gamma^{(0)}(a), 2^{\alpha-2})=2^{\alpha-2-j}，\ 0<\gamma^{(0)}(a)<2^{\alpha-2}.$$

设 $\gamma^{(0)}(a)=2^{\alpha-2-j}\cdot t$，所以上式即 $\left(t, 2^{j}\right)=1, 0<t<2^{j}$．这样的 t 有 $\phi\left(2^{j}\right)=\phi(d)$ 个，由此及 $\gamma^{(-1)}(a)$ 可取 0，1 两个值，所以在一个既约剩余系中指数为 $d(2<d\left|2^{\alpha-2}\right.)$ 的元素恰有 $2\phi(d)$ 个．

例 2 构造模 2^{5} 的以-1 和 5 为底的指标表．

$\gamma^{(-1)}(a)$	0	0	0	0	0	0	0	0	1	1	1	1	1	1	1	1
$\gamma^{(0)}(a)$	0	1	2	3	4	5	6	7	0	1	2	3	4	5	6	7
a	1	5	25	29	17	21	9	13	31	27	7	3	15	11	23	19
$\delta(a)$	1	8	4	8	2	8	4	8	2	8	4	8	2	8	4	8

表 2

以上我们讨论了模 p^{α} 及模 2^{α} 的既约剩余系的情况，下面我们来构造模 m 的既约剩余系．

定理 10 设模 $m=2^{\alpha_0}p_1^{\alpha_1}\cdots p_r^{\alpha_r}, a_i\ge 1(1\le j\le r)$，$p_j(1\le j\le r)$ 是不同的奇素数，g_j 为 $p_j^{\alpha_j}$ 的原根 $(1\le j\le s)$，则

$$\begin{cases} x=M_0M_0^{-1}(-1)^{\gamma^{(-1)}}5^{\gamma^{(0)}}+M_1M_1^{-1}g_1^{\gamma^{(1)}}+\cdots+M_rM_r^{-1}g_r^{\gamma^{(r)}}, \\ 0\le\gamma^{(j)}<c_j,\quad -1\le j\le r, \end{cases}$$

构成模 m 的一组既约剩余系．其中

$$c_{-1}=c_{-1}(\alpha_0)=\begin{cases}1, & \alpha_0=1,\\ 2, & \alpha_0\ge 2,\end{cases}\qquad c_0=c_0(\alpha_0)=\begin{cases}1, & \alpha_0=1,\\ 2^{\alpha_0-2}, & \alpha_0\ge 2,\end{cases},$$

$c_j=\varphi(p_j^{\alpha_j}),\quad 1\le j\le r.\quad m=M_0 2^{\alpha_0}=M_j p_j^{\alpha_j},\ M_j^{-1}M_j\equiv 1(\bmod p_j^{\alpha_j}),\quad (1\le j\le r)$.

此定理利用指标和指标组的概念以及孙子定理很容易证明. 下面我们给出模 m 的指标组的概念.

定义 3 对任意给定的 a，$(a,m)=1$，必有唯一的一组满足定理条件的 $\gamma^{(j)}=\gamma^{(j)}(a)(-1\le j\le r)$ 使得

$$a\equiv M_0M_0^{-1}(-1)^{\gamma^{(-1)}}5^{\gamma^{(0)}}+M_1M_1^{-1}g_1^{\gamma^{(1)}}+\cdots+M_rM_r^{-1}g_r^{\gamma^{(r)}}(\bmod m).$$

我们把

$$\gamma^{(-1)}(a),\gamma^{(0)}(a);\gamma^{(1)}(a),\cdots,\gamma^{(r)}(a)$$

称为是 a 对模 m 的以

$$-1,\ 5;\ g_1,\cdots,\ g_r$$

为底的**指标组**．记为

$$\gamma_m(a)=\{\gamma^{(-1)}(a),\gamma^{(0)}(a);\gamma^{(1)}(a),\cdots,\gamma^{(r)}(a)\}.$$

例 3 求模 $m=2^3\times5^2\times7^2\times11^2$ 的既约剩余系.

解 令 $M_0=5^2\times7^2\times11^2\equiv1(\bmod 2^3)$，$M_0^{-1}\equiv1(\bmod 2^3)$；

$$M_1=2^3\times7^2\times11^2\equiv7(\bmod 5^2),\quad M_1^{-1}\equiv-7(\bmod 5^2);$$

$$M_2=2^3\times5^2\times11^2\equiv-6(\bmod 7^2),\quad M_2^{-1}\equiv8(\bmod 7^2);$$

$$M_3=2^3\times5^2\times7^2\equiv-1(\bmod 11^2),\quad M_3^{-1}\equiv-1(\bmod 11^2).$$

可以验证 $5^2,7^2,11^2$ 的原根分别为 2，3，2．因此

$$x=5^2\times7^2\times11^2\times(-1)^{\gamma^{(-1)}}5^{\gamma^{(0)}}+2^3\times7^2\times11^2\times(-7)\times2^{\gamma^{(1)}}+2^3\times5^2\times11^2\times8\times3^{\gamma^{(2)}}$$
$$+2^3\times5^2\times7^2\times(-1)\times2^{\gamma^{(3)}}(\bmod 2^3\times5^2\times7^2\times11^2)$$

$$0\le\gamma^{(-1)}<2,\quad 0\le\gamma^{(0)}<2,\quad 0\le\gamma^{(1)}<20,\quad 0\le\gamma^{(2)}<42,\quad 0\le\gamma^{(3)}<110.$$

为模 $m=2^3\times5^2\times7^2\times11^2$ 的既约剩余系.

§4 n 次剩余

在上一章提到过二次剩余及 n 次剩余，本节我们来简单介绍一下这方面的知识.

定义 1 设 $m \ge 2,\ (a,m)=1,\ n \ge 2$. 如果同余方程

$$x^n \equiv a(\bmod m), \quad n \ge 2 \tag{1}$$

有解，则称 a 是模 m 的 n 次剩余；如果无解， 则称 a 为是模 m 的 n 次非剩余.

定理 1 设 $m \ge 2,\ (a,m)=1$，模 m 有原根 g，那么同余方程（1）有解，即 a 是模 m 的 n 次剩余的充要条件是

$$(n,\phi(m)) \mid \gamma(a) \tag{2}$$

这里 $\gamma(a)=\gamma_{m,g}(a)$ 是 a 对模 m 的以 g 为底的指标. 此外有解时（1）恰有 $(n,\phi(m))$ 个解.

证明 若 $x \equiv x_1(\bmod m)$ 是（1）的解，由 $(a,m)=1$ 知 $(x_1,m)=1$,

所以，必有 y_1 使得

$$x_1 \equiv g^{y_1}(\bmod m). \tag{3}$$

因而有

$$g^{ny_1} \equiv a(\bmod m) \tag{4}$$

进而由指数的性质知

$$ny_1 \equiv \gamma(a)(\bmod \phi(m)).$$

这表明 $y \equiv y_1(\bmod \phi(m))$ 是一次同余方程

$$ny \equiv \gamma(a)(\bmod \phi(m)) \tag{5}$$

的解. 反过来，若 $y \equiv y_1(\bmod \phi(m))$ 是（5）的解，则同样由§3 性质推出有式（4）成立. 因

此当 x_1 由式（3）给出时，$x \equiv x_1 (\bmod m)$ 必是（1）的解．这就证明了同余方程（1）$((a,m)=1)$ 与同余方程（5）同时有解或无解．此外对任意的

$$x_2 \equiv g^{y_2} (\bmod m),$$

由指数性质（取 $a=g$）知，$x_1 \equiv x_2 (\bmod m)$ 的充要条件是 $y_1 \equiv y_2 (\bmod \phi(m))$．因此，同余方程(1) $((a,m)=1)$ 有解时和同余方程（5）的解数相同．

定理 1 给出了当模 m 有原根时理论上的具体求解方程

$$x^n \equiv a(\bmod m), \quad n \ge 2 \ ((a,m)=1)$$

的方法如下：

（1） 利用指标表找出 a 的指标 $\gamma(a)$；

（2） 解同余方程

$$ny \equiv \gamma(a)(\bmod \phi(m));$$

（3） 若

$$ny \equiv \gamma(a)(\bmod \phi(m))$$

有解，则对每个解 $y_1 (\bmod \phi(m))$ 利用指标表找出 x_1 满足式

$$x_1 \equiv g^{y_1} (\bmod m),$$

这样找到的所有的 $x_1 (\bmod m)$ 就是

$$x^n \equiv a(\bmod m), \quad n \ge 2$$

的全部解．

注 1 我们之所以称上述方法为理论上的求解方法是因为：

（1） 当模 m 为合数时，求 $\phi(m)$ 相当于分解因子问题，理论上可行，但在具体实现时，

被认为是困难问题．例如公钥加密算法 RSA 中，$n = pq$ 是两个大素数的乘积，其安全性基于分解因子是困难问题，无法求出 $\phi(m)$.

（2）　既使 $\phi(m)$ 已知，求 $\gamma(a)$ 即为离散对数问题，我们也认为这是困难的.

注2　若已知 $\phi(m)$，在一种特殊情况下，即 $(\phi(m), n) = 1$ 时，有一种求解

$$x^n \equiv a(\bmod m), \quad n \geq 2$$

的简单方法

$$x = x^{n \cdot n^{-1}(\bmod \phi(m))} = a^{n^{-1}(\bmod \phi(m))}(\bmod m) .$$

例 1 解同余方程 $x^{10} \equiv 13(\bmod 17)$.

解（方法 1） 由第一节知 3 为 17 的原根，查第三节表 1 得 $\gamma_{17,3}(13) = 4$，所以要解同余方程

$$10y \equiv 4(\bmod 16) .$$

由于 $(10, 16) = 2 \mid 4$，所以上述方程有解，它的解为 $y \equiv 2, -6(\bmod 16)$，由第三节表 1 得，指标为 2 的数是 9，指标为-6 的数是 8，因此方程的两个解为 $x \equiv 9,\ 8(\bmod 17)$.

方法 2 先求出 13 模 17 的平方根 ± 8，然后计算 $5^{-1}(\bmod 16) \equiv 13$．故

$$x \equiv x^{5\times 5^{-1}} \equiv (\pm 8)^{13} \equiv \pm 8 \equiv 8, 9(\bmod 17) .$$

模 m 的 n 次剩余有如下性质：

性质 1　设模 m 有原根，$n \geq 2$．那么在模 m 的一个既约剩余系中，模 m 的 n 次剩余恰有 $\phi(m)/(n, \phi(m))$ 个.

性质 2　设模 m 有原根，$n \geq 2$．那么 a 是模 m 的 n 次剩余，即二项同余方程（1）$((a, m) = 1)$ 有解的充要条件是

$$\delta_m(a)\left|\frac{\phi(m)}{(n,\phi(m))}\right.$$

成立，且有解时有$(n,\phi(m))$个解.

证明　当模m有原根时，指数与指标之间有关系

$$\phi(m)=(\phi(m),\gamma(a))\cdot\delta_m(a).$$

因此$(n,\phi(m))\mid\gamma(a)$成立的充要条件是存在整数s使得

$$\frac{\phi(m)}{(n,\phi(m))}=s\cdot\delta_m(a).$$

即

$$\delta_m(a)\mid\frac{\phi(m)}{(n,\phi(m))}.$$

下面来讨论$m=2^a\,(a\geq 3)$的情形.

定理 2　设$m=2^a, a\geq 3, a$是奇数，以及a对模2^a的以$-1,5$为底的指标组是$\gamma^{(-1)}(a),\gamma^{(0)}(a)$.　那么$a$是模$2^a$的$n$次剩余，即二项同余方程（1）有解的充要条件是

$$(n,2)\left|\gamma^{(-1)}(a),\qquad (n,2^{a-2})\right|\gamma^{(0)}(a),\tag{6}$$

且有解时恰有$(n,2)\cdot(n,2^{a-2})$个解，也就是说当n是奇数时，总有解且恰有一解；当n是偶数时，若有解则有$2\cdot(n,2^{a-2})$个解.

证明　由a时奇数知，只要x在模2^a的一个既约剩余系中取值时，讨论方程（1）. 所以可设

$$x=(-1)^u 5^v.\ 0\leq u<2,\ 0\leq v<2^{a-2}.\tag{7}$$

这样，方程（1）就变为一个有两个变数的同余方程

$$\begin{cases}(-1)^{nu}5^{nv}\equiv(-1)^{\gamma^{(-1)}(a)}5^{\gamma^{(0)}(a)}(\operatorname{mod}2^{a}),\\ 0\le u<2,\quad 0\le v<2^{a-2}.\end{cases}\qquad（8）$$

由§3 指数性质知，方程（8），就是同余方程组

$$\begin{cases}nu\equiv\gamma^{(-1)}(a)(\operatorname{mod}2),\qquad 0\le u<2,\\ nv\equiv\gamma^{(0)}(a)(\operatorname{mod}2^{a-2}),\quad 0\le v<2^{a-2}.\end{cases}\qquad（9）$$

由同余方程理论知，第一个一次同余方程（注意u正好在模 2 的一个完全剩余系中取值）有解的充要条件是

$$(n,2)\big|\gamma^{(-1)}(a).\qquad（10）$$

有解时有$(n,2)$个解；第二个一次同余方程（注意v正好是在模2^{a-2}的一个完全剩余系中取值）有解的充要条件是

$$(n,2^{a-2})\big|\gamma^{(0)}(a),\qquad（11）$$

有解时有$(n,2)$个解；所以，同余方程组（9），即同余方程（8），也即同余方程（1）有解的充要条件是式（10），（11）同时成立，即式（6）成立有解时解数应为方程组（9）中两个方程的解数的乘积，即$(n,2)\cdot(n,2^{a-2})$．定理得证.

例 2 解同余方程$x^{7}\equiv 29(\operatorname{mod}2^{5})$.

解 由第 3 节的表 2 知 29 的指标组是$\gamma^{(-1)}(29)=0$，$\gamma^{(0)}(29)=3$因此要解两个一次同余方程

$$\begin{cases}7u\equiv 0(\operatorname{mod}2),\\ 7v\equiv 3(\operatorname{mod}2^{3}),\end{cases}$$

得出

$$\begin{cases}u\equiv 0(\operatorname{mod}2),\\ v\equiv 5(\operatorname{mod}2^{3}),\end{cases}$$

所以$x\equiv(-1)^{0}5^{5}(\operatorname{mod}2^{5})$为方程的解.

练习

1．证明：第 3 节定理 3-5.

2．证明：第 3 节定理 7-8.

3．证明：定理 5 和定理 6.

4．设 $(m_1,m_2)=1$．证明：对任意的 a_1,a_2，必有 a 使得

$$\delta_{m_1m_2}(a)=[\delta_{m_1}(a_1),\delta_{m_2}(a_2)].$$

5．列出 $m=5,11,13,15,19,20$ 的指数表.

6．求 $\delta_{3\times17}(10)$，$\delta_{5\times7}(12)$，$\delta_{5\times13}(14)$，$\delta_{3\times23}(11)$，$\delta_{7^2}(3)$，$\delta_{11^2}(2)$.

7．设 $m>1$，$(ab,m)=1$，及 $\lambda=(\delta_m(a),\delta_m(b))$．证明：

（1）$\lambda^2\delta_m((ab)^\lambda)=\delta_m(a)\delta_m(b)$；

（2）$\lambda^2\delta_m(ab)=(\delta_m(ab),\lambda)\delta_m(a)\delta_m(b)$.

8．设 $m=2^\alpha$，$\alpha\ge4$．证明：$\delta_m(a)=2^{\alpha-2}$ 的充要条件是 $a\equiv\pm3(\bmod 8)$.

9．设素数 $p>2$，$p-1$ 的标准素因数分解式是 $q_1^{\beta_1}\cdots q_r^{\beta_r}$．证明：

（1）　对任一 $j(1\le j\le r)$，存在 a_j 对模 p 的指数是 $q_j^{\beta_j}$（不能利用模 p 存在的原根）;

（2）　$a_1\cdots a_r$ 是模 p 的原根.

10．若 $\delta_m(a)=m-1$，则 m 是素数.

11．设素数 $p\equiv1(\bmod 4)$，若 g 为模 p 的原根，则 $-g$ 也是模 p 的原根.

12．若素数 $p\equiv3(\bmod 4)$，则 g 为模 p 的原根的充要条件是 $\delta_p(-g)=(p-1)/2$.

13．证明：p 是奇素数，$p-1$ 的所有不同的素因数是 $q_1,q_2,\cdots q_s$，那么 g 为模 p 的原根的充要条件是

$$g^{\frac{p-1}{q_j}} \not\equiv 1 \pmod p,\ j = 1, 2, \cdots s .$$

１４．试求模 23，29，41，53，67，73 的原根.

１５．求一个 g 为模 p 的原根，但不是模 p^2 的原根， $p = 5, 7, 11, 13, 17$.

１６．求以 16 为原根的最小素数.

１７．设 $p = 2^{2^k} + 1$为一个素数，试证明：7 是 p 的一个原根的条件.

１８．证明：一定存在 a ，使 $\delta_m(a) = \lambda(m)$ ，且至少有 $\phi(\lambda(m))$ 个两两对模 m 不同余的 a 有这样的性质.

１９．构造模 13，17，19，43，47，61，67 的以最小正原根为底的指标表.

２０．构造 $m = 2^6, 2^7$ 的指标表.

２１．求模 $m = 3\times13\times23\times43$的既约剩余系.

２２．求模 $m = 2^5\times3^2\times13^2$ 的即约剩余系.

２３．求 5 对模 m 的指标组.

（1） $m = 2^6\times17\times23$；

（2） $m = 2^7\times13\times47$.

２４．解同余方程

（1） $3x^6 \equiv 5 \pmod{17}$；

（2） $5x^{12} \equiv -1 \pmod{17}$；

（3） $7x^4 \equiv 8 \pmod{13}$；

（4） $x^{12} \equiv 11 \pmod{13}$；

（5） $x^5 \equiv 12 \pmod{19}$；

（6） $3^x = 2 \pmod{23}$；

（7） $10^x \equiv -7 \pmod{23}$.

２５．当 a 为何值时， $ax^8 \equiv 5 \pmod{17}$ 有解.

２６．设 p 是素数，证明：同余方程 $x^8 \equiv 16 \pmod p$ 一定有解.

２７．设素数 $p > 2$．证明：同余方程 $x^4 \equiv -1 \pmod p$ 有解的充要条件是 $p \equiv 1 \pmod 8$.

２８．解同余方程

（1） $x^4 \equiv 25 \pmod{2^5}$；

（2） $x^{12} \equiv 7 \pmod{128}$.

２９．设 p 是素数，$2 \mid \delta_p(a)$．证明：同余方程 $a^x + 1 \equiv 0 \pmod p$ 无解.

３０．设素数 $p \equiv 3 \pmod 4$．证明：a 是模 p 的四次剩余的充要条件是 $(\frac{a}{p}) = 1$.