第5章 原根与阶

在研究了二次剩余之后,下面讨论 n 次剩余。本章讨论使得同余式 $a^n \equiv 1 \pmod m$ 成立的整数 n。

这里主要关心最小的正整数 e,因为找到了 e,则 e 的倍数均为上式的解。另外,由欧拉定理可知,当 $(a,m)=1$ 时,有 $a^{\varphi(m)} \equiv 1 \pmod m$。于是,这里关心以下问题:这个最小的正整数 e 会不会就是 $\varphi(m)$?在什么情况下它就是 $\varphi(m)$?

本章的重点是原根、阶及其计算方法。难点是 Diffie-Hellman 密钥协商和 ElGamal 公钥密码系统。

5.1 原根与阶的概念

定义 5.1 设 $m>1$ 是整数,a 是正整数,$(a,m)=1$,则使得

$$a^x \equiv 1 \pmod m$$

成立的最小正整数 x 叫作 a 模 m 的阶(order)。记为 $\mathrm{ord}_m(a)$。

例 5.1 设整数 $m=7$,计算 $a=1,2,3,4,5,6$ 的阶。

解:$1^1 \equiv 1 \pmod 7$

$2^3 \equiv 1 \pmod 7$

$3^3 \equiv 1 \pmod 7$

$4^3 \equiv (-3)^3 \equiv 1 \pmod 7$

$5^3 \equiv (-2)^3 \equiv 1 \pmod 7$

$6^2 \equiv (-1)^2 \equiv 1 \pmod 7$

a 模 7 的阶如表 5.1 所示。

表 5.1 a 模 7 的阶

a	1	2	3	4	5	6
$\mathrm{ord}_7(a)$	1	3	6	3	6	2

容易看到,由于 $\varphi(m)=\varphi(7)=6$,于是,$\mathrm{ord}_7(a)$ 中最大的为 6。

定义 5.2 如果 $\mathrm{ord}_m(a)=\varphi(m)$,则 a 叫作 m 的原根(primitive root)。

思考 5.1 原根的英文可能初学者会觉得很难理解,如果称为生成元(generator)可能

更容易理解这个“本原”(primitive)的含义,即可以生成群中其他所有元素的“本原”元。

容易看到,在例5.1中,因为3和5的阶为$\varphi(7)$,所以3和5为原根。

从生成元的角度更加容易理解原根,但需要群的概念。群$(\mathbf{Z}/7\mathbf{Z})^*$中元素的个数为$\varphi(7)=6$,因为3和5的阶为$\varphi(7)$,故3和5可以生成群$(\mathbf{Z}/7\mathbf{Z})^*$中的任意元素(即1～6)。

首先考察3的情况:

$$3^1 \equiv 3 \pmod 7$$
$$3^2 \equiv 2 \pmod 7$$
$$3^3 \equiv 6 \pmod 7$$
$$3^4 \equiv 4 \pmod 7$$
$$3^5 \equiv 5 \pmod 7$$
$$3^6 \equiv 1 \pmod 7$$

容易看到这是一个循环群,3可以生成群中的元素1～6,如图5.1所示。

再考察5的情况:

$$5^1 \equiv 5 \pmod 7$$
$$5^2 \equiv 4 \pmod 7$$
$$5^3 \equiv 6 \pmod 7$$
$$5^4 \equiv 2 \pmod 7$$
$$5^5 \equiv 3 \pmod 7$$
$$5^6 \equiv 1 \pmod 7$$

除了3和5外,其他都不是原根,因为其阶均小于$\varphi(7)$,回到原点1的过程过快,导致只能生成群中的部分元素,无法生成所有元素,

例如,考察2的情况:

$$2^1 \equiv 2 \pmod 7$$
$$2^2 \equiv 4 \pmod 7$$
$$2^3 \equiv 1 \pmod 7$$

容易看到,2无法生成3、5、6。2的阶是3,如图5.2所示。

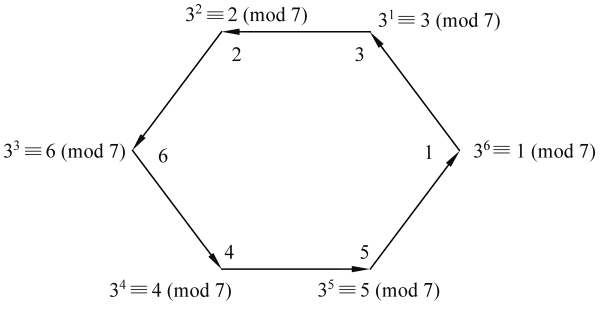

图5.1　3作为生成元生成$(\mathbf{Z}/7\mathbf{Z})^*$中所有元素

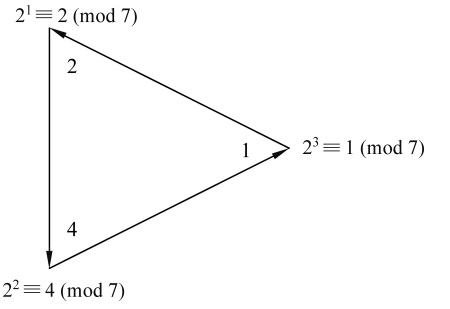

图5.2　2只能生成$(\mathbf{Z}/7\mathbf{Z})^*$中的3个元素

从上述讨论就容易理解为什么原根的阶为$\varphi(m)$了。

下面看一个m不为素数的例子。

例5.2　设整数$m=14$,计算$a=1,3,5,9,11,13$的阶,指出其中的原根。

解：$1^1 \equiv 1 \pmod{14}$

$3^3 \equiv -1 \pmod{14}$

$5^3 \equiv -1 \pmod{14}$

$9^3 \equiv 1 \pmod{14}$

$11^3 \equiv 1 \pmod{14}$

$13^2 \equiv 1 \pmod{14}$

a 模 14 的阶如表 5.2 所示。

表 5.2　a 模 14 的阶

a	1	3	5	9	11	13
$\mathrm{ord}_{14}(a)$	1	6	6	3	3	2

由于 $\varphi(14) = \varphi(2)\varphi(7) = \varphi(7) = 6$，因此原根为 3 和 5。

定理 5.1 给出了计算阶的算法依据。

定理 5.1　设 $m>1$ 是整数，a 为整数，$(a,m) = 1$，则整数 d 使得

$$a^d \equiv 1 \pmod{m}$$

成立的充要条件是

$$\mathrm{ord}_m(a) \mid d$$

证明：先证明充分性。如果 $\mathrm{ord}_m(a) \mid d$，那么存在整数 k，使得 $d = k\,\mathrm{ord}_m(a)$。因此，有

$$a^d = (a^{\mathrm{ord}_m(a)})^k \equiv 1 \pmod{m}$$

再证明必要性。如果 $\mathrm{ord}_m(a) \mid d$ 不成立，则存在整数 q、r，使得

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

从而，

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

又因为

$$a^d \equiv 1 \pmod{m}$$

于是

$$a^r \equiv 1 \pmod{m}$$

这与 $\mathrm{ord}_m(a)$的最小性矛盾。于是有 $\mathrm{ord}_m(a) \mid d$。 ■

推论　设 $m>1$ 是整数，a 为整数，$(a,m) = 1$，则 $\mathrm{ord}_m(a) \mid \varphi(m)$。

证明：根据欧拉定理，有

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

由定理 5.1 可得 $\mathrm{ord}_m(a) \mid \varphi(m)$。 ■

由上述推论可知，可以从 $\varphi(m)$中寻找 $\mathrm{ord}_m(a)$。

例 5.3　求整数 5 模 17 的阶 $\mathrm{ord}_{17}(5)$。

解：因为 $\varphi(17) = 16$，只需要对 16 的因子 $d = 1,2,4,8,16$ 计算 $5^d \pmod{17}$，看是否等于 1。因为

$$5^1 \equiv 5 \pmod{17}$$

$$5^2 \equiv 8 \pmod{17}$$
$$5^4 \equiv 64 \equiv 13 \equiv -4 \pmod{17}$$
$$5^8 \equiv (-4)^2 \equiv 16 \equiv -1 \pmod{17}$$
$$5^{16} \equiv (-1)^2 \equiv 1 \pmod{17}$$

所以5是模17的原根。

有了原根的概念后,可以给出指数的概念。

定义 5.3 设 g 是正整数 m 的原根,若 $\gcd(a,m)=1$,则称同余式

$$g^x \equiv a \pmod{m}$$

的唯一整数解 $x(1\leqslant x\leqslant \varphi(m))$ 为 a 模 m 以 g 为底的指数(index),也称为指标或离散对数,记为 $\mathrm{ind}_{g,m}(a)$,简记为 $\mathrm{ind}_g a$。①

离散对数问题是一个计算上困难的问题,目前还没有找到有效的算法。5.3节和5.4节会给出基于该困难问题构造密码系统。第11章会讲解离散对数算法。

例 5.4 设 $m=7$,由例5.1知,3为原根。计算 $a=1,2,3,4,5,6$ 模7的指数。

解:a 模7的指数如表5.3所示。

表 5.3 a 模 7 的指数

a	1	2	3	4	5	6
$\mathrm{ind}_3 a$	6	2	1	4	5	3

思考 5.2 阶和指数的主要区别是什么?

容易看到,阶与模 m 和整数 a 有关,指数则与模 m、整数 a 以及底(原根 g)有关。阶可以用来判断原根,指数主要用来计算元素相对于原根的离散对数。

定理 5.2(指数定理) 若 g 是模 m 的一个原根,则 $g^x \equiv g^y \pmod{m}$ 当且仅当 $x \equiv y \pmod{\varphi(m)}$。

证明:充分性。假设 $x \equiv y \pmod{\varphi(m)}$,则 $x=y+k\varphi(m)$,$k\in\mathbf{Z}$,所以

$$\begin{aligned} g^x &\equiv g^{y+k\varphi(m)} \pmod{m} \\ &\equiv g^y (g^{\varphi(m)})^k \pmod{m} \\ &\equiv g^y 1^k \pmod{m} \\ &\equiv g^y \pmod{m} \end{aligned}$$

必要性留作练习。 ■

这个证明和RSA的解密过程有相似之处。

定理 5.3 设 g 是模素数 p 的一个原根,且 $\gcd(a,p)=1$,则 $g^k \equiv a \pmod{p}$ 当且仅当

$$k \equiv \mathrm{ind}_g a \pmod{p-1}$$

定理 5.4 设 m 是有原根 g 的正整数,a 与 b 是与 m 相互素的整数。

(1) 若 $b \equiv a \pmod{m}$,则 $\mathrm{ind}_g b \equiv \mathrm{ind}_g a \pmod{\varphi(m)}$。

(2) $\mathrm{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$。

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

① 有些书把ord译为"指数",而用"指标"表示离散对数。本书将ord译为"阶";"指数"和"指标"与离散对数等同,缩写为ind。

(4) $\text{ind}_g a^k \equiv k\ \text{ind}_g a\ (\text{mod}\ \varphi(m))$，$k$ 是一个正整数。

定义 5.4　设 m 是大于 1 的整数，a 是与 m 互素的整数。如果 n 次同余式

$$x^n \equiv a\ (\text{mod}\ m)$$

有解，则 a 叫作模 m 的 n 次剩余；否则，a 叫作模 m 的 n 次非剩余。

定理 5.5　设 m 是大于 1 的整数，g 是模 m 的原根，a 是与 m 互素的整数，则同余式

$$x^n \equiv a\ (\text{mod}\ m)$$

有解的充要条件是

$$(n,\ \varphi(m)) \mid \text{ind}_g a$$

且在有解的条件下解数为$(n,\ \varphi(m))$。

证明：由同余式 $x^n \equiv a\ (\text{mod}\ m)$和$(a,m)=1$，可得$(x,m)=1$，于是以 g 为底的 x 模 m 的指数存在，设为 y，即 $x \equiv g^y (\text{mod}\ m)$，同余式可转换为

$$g^{ny} \equiv a (\text{mod}\ m)$$

由定理 5.5 知

$$ny \equiv \text{ind}_g a (\text{mod}\ \varphi(m))$$

这是关于 y 的一次同余式，根据定理 3.1，其有解的充要条件是$(n,\ \varphi(m)) \mid \text{ind}_g a$，且解数为$(n,\ \varphi(m))$。■

例 5.5　求解同余式 $4^x \equiv 16\ (\text{mod}\ 17)$的所有解。

解：两边取底为 5 的模 17 的指数，得到

$$\text{ind}_5(4^x) \equiv \text{ind}_5 16 \equiv 8\ (\text{mod}\ 16)$$

即

$$\text{ind}_5(4^x) \equiv x\ \text{ind}_5 4 \equiv 12x \equiv 8\ (\text{mod}\ 16)$$

因此

$$12x \equiv 8\ (\text{mod}\ 16)$$

利用一次同余式的解法(定理 3.1)，因为$(12,16)=4$，所以 $12x \equiv 8\ (\text{mod}\ 16)$有 4 个不同余的解，为

$$x \equiv 14,\ 2,\ 6,\ 10\ (\text{mod}\ 16)$$

这即为同余式 $4^x \equiv 16\ (\text{mod}\ 17)$的所有解。

5.2　原根与阶的计算方法

不是所有的模 n 都有原根，定理 5.6 给出了存在原根的条件。

定理 5.6　模 m 的原根存在的充要条件是 $m=2,4,p^\alpha,2p^\alpha$，其中 p 是奇素数，α 是一个正整数。

定理 5.6 的证明要点如下：

(1) 每个素数都有原根。

(2) 奇素数的幂都有原根。

(3) 在 2 的幂中，只有 2 和 4 有原根。

(4) 被两个或者更多素数整除的整数中，只有那些奇素数的幂的 2 倍的整数才有原根。

证明从略。

定理 5.7 设 $m>1$,$\varphi(m)$的所有不同素因子是 q_1, q_2, …, q_k,则 g 是模 m 的一个原根的充要条件是

$$g^{\varphi(m)/q_i} \not\equiv 1 \pmod{m}, \quad i=1,2,\cdots,k$$

证明:先证明必要性。设 g 是模 m 的一个原根,则 g 模 m 的阶是 $\varphi(m)$。但是

$$0 < \varphi(m)/q_i < \varphi(m), \quad i=1,2,\cdots,k$$

由原根的定义知

$$g^{\varphi(m)/q_i} \not\equiv 1 \pmod{m}, \quad i=1,2,\cdots,k$$

再证明充分性。

若 g 模 m 的阶 $e<\varphi(m)$,则根据定理 5.1 的推论,有 $e\mid\varphi(m)$,于是存在一个素数 q,使得 $q \mid (\varphi(m)/e)$。于是,根据整除的定义,存在一个整数 u,有

$$qu=\frac{\varphi(m)}{e}$$

即

$$eu=\frac{\varphi(m)}{q}$$

于是

$$g^{\varphi(m)/q}=(g^e)^u \equiv 1 \pmod{m}$$

这与假设矛盾。 ■

定理 5.7 给出了求原根的算法的基础。

其实定理 5.7 的逻辑很简单,通俗地说,就是不要提前回到 1。如果 $g^{\varphi(m)/q_i}$ 模 m 不等于 1,说明 $g^{\prod_{j\neq i} q_j}$ 模 m 不等于 1,从而也说明 $g^{q_j}(j\neq i)$模 m 也不等于 1。

例 5.6 求 41 的一个原根。

解:$\varphi(41)=40=2^3\times5$,素因子为 2 和 5。$\varphi(41)/2=20$,$\varphi(41)/5=8$。因此,只需要验证 g^8、g^{20}模 m 是否同余于 1。对于 2,3,4,…,逐个验算:

$$2^8 \equiv 10 \pmod{41}, \quad 2^{20} \equiv 1 \pmod{41}$$
$$3^8 \equiv 1 \pmod{41}, \quad 4^8 \equiv 18 \pmod{41}$$
$$4^{20} \equiv 1 \pmod{41}, \quad 5^8 \equiv 18 \pmod{41}$$
$$5^{20} \equiv 1 \pmod{41}, \quad 6^8 \equiv 10 \pmod{41}$$
$$6^{20} \equiv 40 \pmod{41}$$

因此,6 是模 41 的原根。

定理 5.8 设 $m>1$ 的整数,a 为整数且$(a,m)=1$,$d\geqslant0$ 为整数,则

$$a^d \equiv a^k \pmod{m}$$

的充要条件是

$$d \equiv k \pmod{\mathrm{ord}_m(a)}$$

证明:根据欧几里得除法,存在整数 q、r 和 q'、r'有

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

又 $a^{\mathrm{ord}_m(a)}\equiv1 \pmod{m}$,于是

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

$$a^k \equiv a^{\mathrm{ord}_m(a)q'} a^{r'} \equiv a^{r'} \pmod m$$

必要性。若 $a^d \equiv a^k \pmod m$，则 $a^r \equiv a^{r'} \pmod m$，于是 $r = r'$，有 $d \equiv k \pmod{\mathrm{ord}_m(a)}$。

以上步步可逆，知充分性。 ■

例 5.7　因为整数 2 模 7 的阶为 $\mathrm{ord}_7(2)=3$，$2015 \equiv 2 \pmod 3$，因此，

$$2^{2015} \equiv 2^2 \pmod 7$$

在 2.1 节中例 2.1 曾经给出一个实际的应用例子。

定理 5.9　设 $m>1$ 为整数，a 为整数且 $(a,m)=1$，$d \geqslant 0$ 为整数，则

$$\mathrm{ord}_m(a^d) = \frac{\mathrm{ord}_m(a)}{(\mathrm{ord}_m(a), d)}$$

具体证明从略，读者可尝试完成。

证明主要在于阶的定义，即寻找使得 $(a^d)^x$ 模 m 等于 1 的最小幂次 x。容易看到 $x = \mathrm{ord}_m(a)$ 是一种可能，但是偏大。$x = \mathrm{ord}_m(a)$ 可缩小（即除以 d 和 $\mathrm{ord}_m(a)$ 的最大公约数，$x = \dfrac{\mathrm{ord}_m(a)}{(\mathrm{ord}_m(a), d)}$）后，依然可以使得 a^d 在 x 幂次后模 m 等于 1。如果 x 进一步缩小，则必然有些因子在 $\mathrm{ord}_m(a)$ 里而不在 d 里，导致 dx 缺少这一因子而不能整除 $\mathrm{ord}_m(a)$，从而 $a^{dx} \neq 1 \pmod m$。

思考 5.3　如何利用图 5.1 和图 5.2 给出一个对定理 5.9 的直观解释？

如图 5.3 所示。通俗地说，以原根 3 为度量，$2 = 3^2 \pmod 7$，视为 2“行走”1 步相当于 3“行走”2 步，于是对于 2 而言，“行走”一周（6 步）就需要 6/2=3 步，即 $\mathrm{ord}_7(2)=3$。

如果“行走”1 步相当于 3“行走”3 步（例如 6），则“行走”一周需要 6/3=2 步（即 6 的阶是 2）。

如果“行走”1 步相当于 3“行走”4 步（例如 4），则“行走”一周需要 6/(6,4)=6/2=3 步（即 4 的阶是 3）。

如果“行走”1 步相当于 3“行走”5 步（例如 5），则“行走”一周需要 6/(6,5)=6/1=6 步（即 5 的阶是 6）。

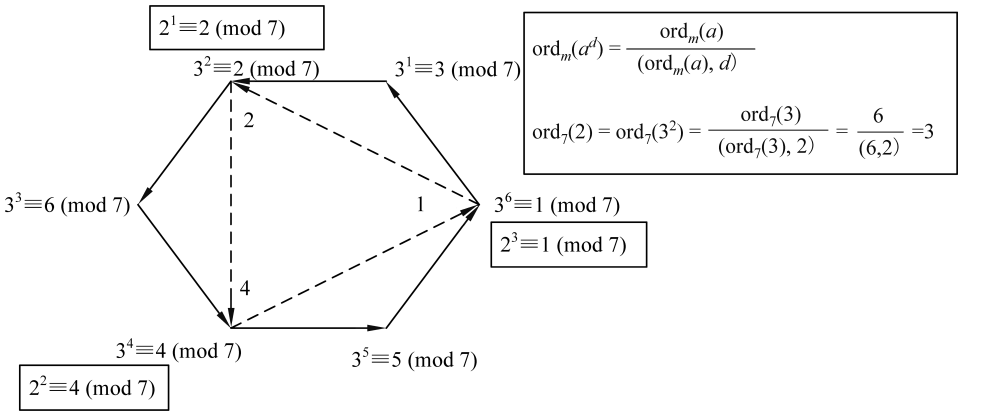

图 5.3　定理 5.9 的直观解释

推论 1　设 $m>1$ 是整数，g 是模 m 的原根，$d \geqslant 0$ 为整数，则 g^d 是模 m 的原根当且仅

当$(d,\varphi(m))=1$。

推论2 设$m>1$是整数,m有$\varphi(\varphi(m))$个不同的原根。

例如,设素数$p=47$,则存在$\varphi(47-1)=22$个模47的原根。

目前还没有一种方法可以预知一个给定素数p的最小原根,对$\varphi(p-1)$个原根在模p的最小剩余系中的分布也知之甚少。

下面给出一个十分精美的定理。

定理5.10 设n为一个正整数,则

$$n=\sum_{d|n}\varphi(d)$$

证明:令C_d为1到n中与n的最大公约数为d的整数m的集合,即

$$C_d=\{m \mid m\in[1,n],(m,n)=d\}$$

易知

$$|C_d=\{m \mid m\in[1,n],(m/d,n/d)=1\}|=|\{t \mid 1\leqslant t\leqslant n/d,(t,n/d)=1\}|$$

这恰好就是$\varphi(n/d)$。由于每个1到n的整数m必然属于一个且只属于一个集合,故

$$n=\sum_{d|n}\varphi(n/d)$$

因为d遍历n的所有正因子时n/d也遍历n的所有正因子,所以

$$n=\sum_{d|n}\varphi(n/d)=\sum_{d|n}\varphi(d)$$ ■

以图5.3为例,$n=7-1=6$,$d=1,2,3,6$,$C_6=\{6\}$,$C_3=\{3\}$,$C_2=\{2,4\}$,$C_1=\{1,5\}$,6个整数分别属于且只属于一个集合。

$$|C_6|=\varphi(6/6)=\varphi(1)=1$$
$$|C_3|=\varphi(6/3)=\varphi(2)=1$$
$$|C_2|=\varphi(6/2)=\varphi(3)=2$$
$$|C_1|=\varphi(6/1)=\varphi(6)=2$$

定理5.9给出了从一个原根求其他原根的算法基础。

例5.8 已知6是41的原根,求41的所有原根。

解:由定理5.5知,$(d,\varphi(41))=1$时,$\mathrm{ord}_{41}(g^d)=\mathrm{ord}_{41}(g)$,因此,当$d$遍历模$\varphi(41)=40$的简化剩余系,即1,3,7,9,11,13,17,19,21,23,27,29,31,33,37,39共$\varphi(\varphi(41))=16$个数时,6^d遍历41的所有原根。即

$6^1\equiv 6\pmod{41}$, $6^3\equiv 11\pmod{41}$, $6^7\equiv 29\pmod{41}$, $6^9\equiv 19\pmod{41}$,
$6^{11}\equiv 28\pmod{41}$, $6^{13}\equiv 24\pmod{41}$, $6^{17}\equiv 26\pmod{41}$, $6^{19}\equiv 34\pmod{41}$,
$6^{21}\equiv 35\pmod{41}$, $6^{23}\equiv 30\pmod{41}$, $6^{27}\equiv 12\pmod{41}$, $6^{29}\equiv 22\pmod{41}$,
$6^{31}\equiv 13\pmod{41}$, $6^{33}\equiv 17\pmod{41}$, $6^{37}\equiv 15\pmod{41}$, $6^{39}\equiv 7\pmod{41}$

定理5.7和定理5.9构成了求原根的算法基础。

算法5.1 GetPrimitiveRoot()
输入:素数模m,以及$m-1$的素因子分解$m-1=p_1^{c1}\ p_2^{c2}\cdots p_k^{ck}$
输出:m的所有原根
1. 随机选择一个数a,$2\leqslant a\leqslant m-1$

2. 对 i 从 1 到 k 执行如下计算：
　计算 $b \leftarrow a^{(m-1)/p_i} \pmod m$
　如果 $b=1$ 则转到步骤 1
3. 对 d 从 1 到 $m-1$ 执行如下计算：
　若 $\gcd(d, m-1)=1$，则输出 $a^d \pmod m$

思考 5.4　根据定理 5.9 给出求阶表的算法。输入为素数模和原根，输出为阶表。

算法 5.2　GetOrder()
输入：素数模 m，原根 a
输出：阶表
对 i 从 1 到 $m-1$ 执行如下计算：
　return $a^i \pmod m$，$(m-1)/\gcd(m-1,i)$

定理 5.11　设 $m>1$ 是整数，a 为整数且 $(a,m)=1$。
(1) 设 a^{-1} 使得 $a^{-1}a \equiv 1 \pmod m$，则 $\mathrm{ord}_m(a^{-1}) = \mathrm{ord}_m(a)$。
(2) 若 $b \equiv a \pmod m$，则 $\mathrm{ord}_m(b) = \mathrm{ord}_m(a)$。

证明：
(1) 因为 $(a^{-1})^{\mathrm{ord}_m(a)} \equiv (a^{\mathrm{ord}_m(a)})^{-1} \equiv 1 \pmod m$
因此，$\mathrm{ord}_m(a^{-1}) \mid \mathrm{ord}_m(a)$。
同理可证 $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(a^{-1})$，于是有 $\mathrm{ord}_m(a^{-1}) = \mathrm{ord}_m(a)$。
(2) 若 $b \equiv a \pmod m$，则

$$b^{\mathrm{ord}_m(a)} \equiv a^{\mathrm{ord}_m(a)} \equiv 1 \pmod m$$

于是 $\mathrm{ord}_m(b) \mid \mathrm{ord}_m(a)$。
同理可证 $\mathrm{ord}_m(a) \mid \mathrm{ord}_m(b)$，于是 $\mathrm{ord}_m(b) = \mathrm{ord}_m(a)$。 ■

定理 5.11 的结论(1)也可以从图 5.3 中得到直观的解释。3 和 5 互为逆元，5 相当于“反着行走”了一圈(如图 5.4 所示)。因为 5“行走”1 步到 5，5“行走”2 步到 4……5“行走”6 步到 1，所以 5 的阶为 6。

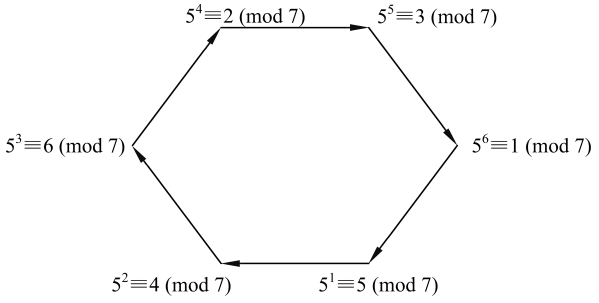

图 5.4　对定理 5.11 的直观解释

同理，2 和 4 互为逆元。读者也可以画出类似的示意图。
定理 5.12 将原根，阶，以及简化剩余系等概念联系到一起。
定理 5.12　设 $m>1$ 是整数，a 为整数且 $(a,m)=1$，则

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

模 m 两两不同余。特别地,当 a 是模 m 的原根,即 $\mathrm{ord}_m(a)=\varphi(m)$时,这 $\varphi(m)$个数组成模 m 的简化剩余系。

证明:反证法。如果 $\mathrm{ord}_m(a)$个数中有两个数模 m 同余,则存在整数 $0\leqslant k,l\leqslant \mathrm{ord}_m(a)$ 使得

$$a^k\equiv a^l(\mathrm{mod}\ m)$$

不妨设 $k>l$,则由$(a,m)=1$ 和定理 2.4,得到

$$a^{k-l}\equiv 1\ (\mathrm{mod}\ m)$$

但是 $0\leqslant k,l\leqslant \mathrm{ord}_m(a)$,这与 $\mathrm{ord}_m(a)$的最小性矛盾。因此,原结论成立。

当 a 为原根时,即 $\mathrm{ord}_m(a)=\varphi(m)$时,共有 $\varphi(m)$个数:

$$1=a^0,a^1,\cdots,a^{\varphi(m)-1}$$

且模 m 两两不同余,由定理 2.8 知,这 $\varphi(m)$个数组成模 m 的简化剩余系。 ■

在第 6 章将看到,模 m 的简化剩余系构成一个乘法群,其生成元为 a,a 生成了这个群中的所有元素。这个群其实还是一个循环群。

5.3 Diffie-Hellman 密钥协商协议

原根和指数,尤其是循环群的原根,在密码学中有重要的应用。例如,基于离散对数问题的 Diffie-Hellman 密钥协商协议,以及基于 Diffie-Hellman 密钥协商协议的 ElGamal 公钥加密系统。

在定义 2.7 的说明中曾经指出,对称密码中加密密钥和解密密钥是相同的,因此,对称密码的困难之处有两点:

(1) 密钥的管理。对称加密中加密解密双方使用相同的密钥,每一对加密方和解密方就需要一个密钥,而且密钥必须保密,因此对密钥的存储和管理难度较大。

(2) 当加密方和解密方在不同地理位置时,通信双方如何确定一个秘密密钥,或者通信发送方如何将秘密密钥传递给通信接收方,都是难以解决的问题。

思考 5.5 对于共有 n 个通信方的两两通信,需要多少秘密密钥?

对称密码需要的密钥数量:对单个通信方而言,需要保存 $n-1$ 个秘密密钥;对总体而言,需要保存 $n(n-1)/2$ 个秘密密钥。

定义 3.2 指出,公钥密码使用公开的公钥进行加密和保密的私钥进行解密。需要的密钥数量:对单个通信方而言,需要保存 n 个公钥和一个私钥;对总体而言,需要保存 n 个公钥和 n 个私钥。所需密钥的数量减少,而且需要秘密保存的密钥数量大为减少。

因此,需要解决的一个安全问题是:在公开信道上如何协商一个秘密密钥,用于后续的对称密码加密通信。

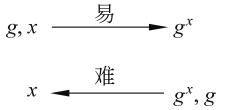

图 5.5 离散对数问题中的单向性

W. Diffie 与 M. Hellman 利用离散对数问题的困难性,在 1976 年提出了 Diffie-Hellman 密钥协商协议。

首先看离散对数问题中的单向性,如图 5.5 所示。

设 G 是生成元为 g 的 n 阶循环群。