第3章　原　　根

【教学目的】

掌握指数与原根的基本概念；能够利用指数的计算技巧寻找原根；能够利用原根的性质计算指数，能够建立离散对数表求解高次同余方程。

【教学要求】

通过本章的学习，读者能够：

(1) 识记：指数与原根等基本概念和性质，原根的存在条件。

(2) 领会：各定理如何优化原根的寻找过程。

(3) 简单应用：利用指数计算技巧寻找一个原根，利用一个原根生成缩系中的所有元素，利用一个原根计算缩系中各元素的指数，建立离散对数表求解高次同余方程。

(4) 综合应用：高次同余方程求解的程序实现，离散对数密码的设计与实现。

【学习重点与难点】

本章重点与难点是：利用指数计算技巧寻找原根，利用原根性质计算各数指数，求解高次同余方程等问题。

代数最主要的问题是解方程，在第2章中已经学习过解一次同余方程，本章围绕的是解高阶指数方程。在正式开始本章学习之前，请思考下面这三个问题。

(1) 根据欧拉定理知道 $2^6\equiv 1 \pmod 7$，其实 $2^3\equiv 1 \pmod 7$，显然后者对于幂指数化简更有价值。如根据欧拉定理有 $2^{22}\equiv 2^4 \pmod 7$；实际上可以根据 $2^3\equiv 1 \pmod 7$ 将其化简成更简单的形式 $2^{22}\equiv 2 \pmod 7$。

那么，你能不能对模 $m=17、27、37、47、67、87\cdots$ 类似地找到比欧拉函数更小的数字 k，使得 $2^k\equiv 1 \pmod m$？

(2) 根据欧拉定理知道 $2^6\equiv 1 \pmod 7$，考虑中间的计算过程：

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

因此，$2^k \pmod 7$ 实际上会形成一个周期为3的循环。对于3则有：

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

因此，$3^k \pmod 7$ 实际上会形成一个周期为6的循环。那么若底数为4、5、6呢？这其中体现了什么样的规律？

(3) 在中学曾经学过 $2^x=1000$ 的解为 $x=\log_2 1000$；$x^2=1000$ 的解为 $2\log_{10}|x|=\log_{10}1000=3$，所以 $x=\pm 10^{3/2}$。你能不能类似地求解 $2^x=1000 \pmod 7$ 和 $x^2=1000 \pmod 7$？这与中学的指数方程和对数方程求解有什么异同？

上述问题都围绕着本章的核心：原根。利用原根的性质可以快速地实现加密，为了使加密结果直观可见，将图3-1(a)的lena图像分成6块，使用 $y\equiv 3^x \pmod 7$，就可以加密成图3-1(b)，实现了换位式密码，其中，x 表示原始图像块标号，y 表示加密后图像块标号。

(a) 原始lena图像X　　(b) 加密后lena图像Y

图 3-1　简单换位式加密算法示意图

3.1　指数

定义 3.1　指数

$m,a\in\mathbf{Z},m>1,(a,m)=1$，使 $a^k\equiv1\pmod m$ 成立的**最小正整数 k**，称为 a 模 m 的指数，记为 $\mathrm{ord}_m(a)$。

例 3.1　$\mathrm{ord}_m(1)=1$，　$\mathrm{ord}_7(3)=6$，　$\mathrm{ord}_7(2)=3$，

$\mathrm{ord}_2(-1)=1$，　$\mathrm{ord}_m(-1)=2\ (m>2)$。

【请你注意】

(1) 如果$(a,m)>1$，则规定 $\mathrm{ord}_m(a)=0$；

(2) 在谈到 a 对模 m 的指数时，总假定 $m>1,(a,m)=1$；

(3) 指数有时也称为阶，与 $\mathrm{ord}_m(a)$等同的符号是$\delta_m(a)$。

例 3.2　请计算 $\mathrm{ord}_7(5)$。

解：因为 $5^1\equiv5,5^2\equiv4,5^3\equiv6,5^4\equiv2,5^5\equiv3,5^6\equiv1\pmod7$，所以 $\mathrm{ord}_7(5)=6$。

相似地，可以得出：

$1^1\equiv1\pmod7$；

$2^1\equiv2,2^2\equiv4,2^3\equiv8\equiv1\pmod7$；

$3^1\equiv3,3^2\equiv2,3^3\equiv27\equiv-1,3^4\equiv-3,3^5\equiv-12\equiv5,3^6\equiv1\pmod7$；

$4^1\equiv4,4^2\equiv16\equiv2,4^3\equiv8\equiv1\pmod7$；

$6^1\equiv6\equiv-1,6^2\equiv1\pmod7$。

从而可以写出模 7 的指数表，如表 3-1 所示。

表 3-1　模 7 指数表

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

观察模 7 的指数表，可以看出：a 有 $\varphi(7)=6$ 个不同的取值，2 与 4 模 7 的指数相同，3 与 5 模 7 的指数相同，所有 a 模 7 的指数都是 $\varphi(7)=6$ 的因数；模 7 的指数是 6 的数字有两

个，模 7 的指数是 3 的数字有两个，模 7 的指数是 2 的数字有一个，模 7 的指数是 1 的数字有一个。

类似地，可以求出模 10 的指数表，如表 3-2 所示。

$1^1 \equiv 1 \pmod{10}$，

$3^1 \equiv 3, 3^2 \equiv 9 \equiv -1, 3^3 \equiv 7, 3^4 \equiv 1 \pmod{10}$，

$7^1 \equiv 7, 7^2 \equiv 9, 7^3 \equiv 3, 7^4 \equiv 1 \pmod{10}$，

$9^1 \equiv 9 \equiv -1, 9^2 \equiv 1 \pmod{10}$。

表 3-2　模 10 指数表

a	1	3	7	9
$\mathbf{ord}_{10}(a)$	1	4	4	2

其中，a 有 $\varphi(10)=4$ 个不同的取值，3 与 7 模 10 的指数相同，所有 a 模 10 的指数都是 $\varphi(10)=4$ 的因数。模 10 的指数是 4 的数字有两个，模 10 的指数是 2 的数字有一个，模 10 的指数是 1 的数字有一个。

同理，模 14 的指数表如表 3-3 所示。

表 3-3　模 14 指数表

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

其中，a 有 $\varphi(14)=6$ 个不同的取值，3 与 5 模 14 的指数相同，9 与 11 模 14 的指数相同，所有 a 模 14 的指数都是 $\varphi(14)$的因数。模 14 的指数是 6 的数字有两个，模 14 的指数是 3 的数字有两个，模 14 的指数是 2 的数字有一个，模 14 的指数是 1 的数字有一个。

归纳起来，指数具有一些基本性质。

定理 3.1　$a, m, n \in \mathbf{Z}, m>1, (a,m)=1, a^n \equiv 1 \pmod{m} \Leftrightarrow \mathrm{ord}_m(a) \mid n$

证明：设 $n=\mathrm{ord}_m(a)q+r, 0 \leqslant r < \mathrm{ord}_m(a), q, r \in \mathbf{Z}$ 则：

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

因为 $\mathrm{ord}_m(a)$ 是满足 $a^k \equiv 1 \pmod{m}$成立的最小正整数，$0 \leqslant r < \mathrm{ord}_m(a)$，

所以 $a^n \equiv 1 \pmod{m} \Leftrightarrow a^r \equiv 1 \pmod{m} \Leftrightarrow r=0$，

即 $a^n \equiv 1 \pmod{m} \Leftrightarrow \mathrm{ord}_m(a) \mid n$。证毕。

推论 3.1　$a, m \in \mathbf{Z}, m>1, (a,m)=1$，有 $\mathrm{ord}_m(a) \mid \varphi(m)$。

定义 3.2　原根

$a, m \in \mathbf{Z}, m>1, (a,m)=1$，若 $\mathbf{ord}_m(a)=\varphi(m)$，则称 a 为模 m 的原根。

如根据模 7 的指数表，3 和 5 是模 7 的原根，1、2、4 和 6 不是模 7 的原根。同理，3 和 7 是模 10 的原根，3 和 5 是模 14 的原根。

例 3.3　请计算 $\mathrm{ord}_{17}(5)$。

解：因为 $\varphi(17)=16$，所以 $\mathrm{ord}_{17}(5) \mid 16$，所以 $\mathrm{ord}_{17}(5)$可能为 1、2、4、8、16，

因为 $5^1 \equiv 5, 5^{16} \equiv 1 \pmod{17}$，所以只需计算 5^2、5^4、$5^8 \pmod{17}$，

因为 $5^2 \equiv 8, 5^4 \equiv 64 \equiv 13, 5^8 \equiv 169 \equiv -1 \pmod{17}$，

所以 $\mathrm{ord}_{17}(5)=16$，即 5 是模 17 的原根。

定理 3.2 $m,a,b\in\mathbf{Z},m>1,(a,m)=1$,

(1) 若 $a\equiv b\pmod m$,则 $\mathrm{ord}_m(a)=\mathrm{ord}_m(b)$;

(2) $ab\equiv1\pmod m$,则 $\mathrm{ord}_m(a)=\mathrm{ord}_m(b)$;

(3) 若 $l,n\in\mathbf{Z},a^n\equiv a^l\pmod m$,则 $n\equiv l\pmod{\mathrm{ord}_m(a)}$;

(4) 记 $n=\mathrm{ord}_m(a)$,则 $a^0,a^1,\cdots,a^{n-1}$模 m 两两不同余,特别地,

a 是原根 $\Leftrightarrow a^0,a^1,\cdots,a^{\varphi(m)-1}$是模 m 的缩系;

(5) 若 $n\mid m$,则 $\mathrm{ord}_n(a)\mid\mathrm{ord}_m(a)$;

(6) 若$(m,n)=1,(a,mn)=1$,则 $\mathrm{ord}_{mn}(a)=[\mathrm{ord}_m(a),\mathrm{ord}_n(a)]$;

(7) 若$(ab,m)=1,(\mathrm{ord}_m(a),\mathrm{ord}_m(b))=1$,则 $\mathrm{ord}_m(ab)=\mathrm{ord}_m(a)\mathrm{ord}_m(b)$。

证明:(1) 因为 $a^{\mathrm{ord}m(a)}\equiv b^{\mathrm{ord}m(a)}\equiv1\pmod m$,所以根据定理 3.1,$\mathrm{ord}_m(b)\mid\mathrm{ord}_m(a)$,

同理:$\mathrm{ord}_m(a)\mid\mathrm{ord}_m(b)$,所以 $\mathrm{ord}_m(a)=\mathrm{ord}_m(b)$。

(2) 因为 $a^{\mathrm{ord}m(a)}\equiv1\pmod m$,所以 $b^{\mathrm{ord}m(a)}\equiv(ab)^{\mathrm{ord}m(a)}\equiv1^{\mathrm{ord}m(a)}\equiv1\pmod m$,

所以 $\mathrm{ord}_m(b)\mid\mathrm{ord}_m(a)$,

同理,$a^{\mathrm{ord}m(b)}\equiv(ab)^{\mathrm{ord}m(b)}\equiv1^{\mathrm{ord}m(b)}\equiv1\pmod m$,所以 $\mathrm{ord}_m(a)\mid\mathrm{ord}_m(b)$,

所以 $\mathrm{ord}_m(a)=\mathrm{ord}_m(b)$。

(3) 不妨设 $n>l$,因为$(a,m)=1$,所以 $a^{n-l}\equiv a^{l-l}\equiv1\pmod m$,

根据定理 3.1,$\mathrm{ord}_m(a)\mid n-l$,即 $n\equiv l\pmod{\mathrm{ord}_m(a)}$。

(4) (反证法)若 $0\leqslant i<j\leqslant n-1$,有 $a^i\equiv a^j\pmod m$,

由(3)得 $j\equiv i\pmod n$,因为 $j-i<n$,所以 $j-i=0$,矛盾,

所以 $a^0,a^1,\cdots,a^{n-1}$对模 m 两两不同余;

若 a 是原根,则 $\mathrm{ord}_m(a)=\varphi(m)$,

所以 $a^0,a^1,\cdots,a^{\varphi(m)-1}$这 $\varphi(m)$个数模 m 两两不同余,

所以 $a^0,a^1,\cdots,a^{\varphi(m)-1}$是模 m 的缩系。

(5) 因为 $a^{\mathrm{ord}m(a)}\equiv1\pmod m$,所以 $a^{\mathrm{ord}m(a)}\equiv1\pmod n$,所以 $\mathrm{ord}_n(a)\mid\mathrm{ord}_m(a)$。

(6) 因为$(m,n)=1,(a,mn)=1$,所以 $\mathrm{ord}_m(a)\mid\mathrm{ord}_{mn}(a),\mathrm{ord}_n(a)\mid\mathrm{ord}_{mn}(a)$,

设 $s=[\mathrm{ord}_m(a),\mathrm{ord}_n(a)]$,所以 $s\mid\mathrm{ord}_{mn}(a)$,

又因为 $\mathrm{ord}_m(a)\mid s,\mathrm{ord}_n(a)\mid s$,所以 $a^s\equiv1\pmod m,a^s\equiv1\pmod n$,

所以 $a^s\equiv1\pmod{mn}$,所以 $\mathrm{ord}_{mn}(a)\mid s$,所以 $\mathrm{ord}_{mn}(a)=[\mathrm{ord}_m(a),\mathrm{ord}_n(a)]$。

(7) 因为 $a^{\mathrm{ord}m(a)\mathrm{ord}m(ab)}\equiv(ab)^{\mathrm{ord}m(ab)\mathrm{ord}m(a)}\equiv1\pmod m$,

所以$(ab)^{\mathrm{ord}m(a)\mathrm{ord}m(ab)}\equiv a^{\mathrm{ord}m(a)\mathrm{ord}m(ab)}\,b^{\mathrm{ord}m(a)\mathrm{ord}m(ab)}\equiv b^{\mathrm{ord}m(a)\mathrm{ord}m(ab)}\equiv1\pmod m$,

所以 $\mathrm{ord}_m(b)\mid\mathrm{ord}_m(ab)\mathrm{ord}_m(a)$,因为$(\mathrm{ord}_m(a),\mathrm{ord}_m(b))=1$,

所以 $\mathrm{ord}_m(b)\mid\mathrm{ord}_m(ab)$,

同理,$\mathrm{ord}_m(a)\mid\mathrm{ord}_m(ab)\mathrm{ord}_m(b)$,所以 $\mathrm{ord}_m(a)\mid\mathrm{ord}_m(ab)$,

所以 $\mathrm{ord}_m(a)\ \mathrm{ord}_m(b)\mid\mathrm{ord}_m(ab)$,

另一方面,$(ab)^{\mathrm{ord}m(a)\mathrm{ord}m(b)}\equiv a^{\mathrm{ord}m(a)}b^{\mathrm{ord}m(b)}\equiv1\pmod m$,

所以 $\mathrm{ord}_m(ab)\mid\mathrm{ord}_m(a)\ \mathrm{ord}_m(b)$,所以 $\mathrm{ord}_m(ab)=\mathrm{ord}_m(a)\ \mathrm{ord}_m(b)$。

例 3.4 请计算 $\mathrm{ord}_{17}(39)$。

解:因为 $39\equiv5\pmod{17}$,所以 $\mathrm{ord}_{17}(39)=\mathrm{ord}_{17}(5)=16$。

例 3.5 请计算 $\mathrm{ord}_{17}(7)$。

解:因为 $7\times5\equiv1\pmod{17}$,所以 $7\equiv5^{-1}\pmod{17}$, 所以 $\mathrm{ord}_{17}(7)=\mathrm{ord}_{17}(5)=16$。

例 3.6 请计算 $2^{211} \pmod 7$。

解：因为 $\mathrm{ord}_7(2)=3$，所以 $2^{211} \pmod 7 \equiv 2^{211 \pmod 3} \pmod 7 \equiv 2 \pmod 7$。

例 3.7 请写出模 10 的缩系。

解：因为 $\varphi(10)=\varphi(2)\ \varphi(5)=1\times 4=4$，$\mathrm{ord}_{10}(3)=4$，所以 3 是模 10 的原根，

所以模 10 的缩系为 $3^0, 3^1, 3^2, 3^3 \pmod{10}$，即 1，3，9，7。

例 3.8 请计算 $\mathrm{ord}_{49}(3)$。

解：因为 $\varphi(49)=7^2-7=42$，所以 $\mathrm{ord}_{49}(3) \mid 42$，所以 $\mathrm{ord}_{49}(3)$ 可能为 1、2、3、6、7、14、21、42，又因为 $\mathrm{ord}_7(3)=6 \mid \mathrm{ord}_{49}(3)$，所以 $\mathrm{ord}_{49}(3)$ 只可能为 6 或 42，

所以只需计算 $3^6 \pmod{49}$，因为 $3^6 \equiv -6 \pmod{49}$，所以 $\mathrm{ord}_{49}(3)=42$。

例 3.9 请计算 $\mathrm{ord}_{28}(3)$。

解：因为 $\varphi(28)=\varphi(4\times 7)=\varphi(4)\times\varphi(7)=2\times 6=12$，所以 $\mathrm{ord}_{28}(3) \mid 12$

(法一)因为 $\mathrm{ord}_7(3) \mid \mathrm{ord}_{28}(3)$，$\mathrm{ord}_4(3) \mid \mathrm{ord}_{28}(3)$，而 $\mathrm{ord}_7(3)=6$，$\mathrm{ord}_4(3)=2$，

所以 $6 \mid \mathrm{ord}_{28}(3)$，　　所以 $\mathrm{ord}_{28}(3)$ 可能为 6 或 12，

因为 $3^6 \equiv 1 \pmod{28}$，　　所以 $\mathrm{ord}_{28}(3)=6$。

(法二)因为 $(4,7)=1$，所以 $\mathrm{ord}_{28}(3)=[\mathrm{ord}_7(3), \mathrm{ord}_4(3)]=[6,2]=6$。

例 3.10 请计算 $\mathrm{ord}_{2904}(5)$。

解：因为 $2904=8\times 3\times 121=2^3\times 3\times 11^2$，所以首先计算 $\mathrm{ord}_8(5)$，$\mathrm{ord}_3(5)$ 和 $\mathrm{ord}_{121}(5)$，

因为 $\varphi(8)=8-4=4$，$5^2 \equiv 1 \pmod 8$，所以 $\mathrm{ord}_8(5)=2$，

因为 $5 \equiv -1 \pmod 3$，所以 $\mathrm{ord}_3(5)=\mathrm{ord}_3(-1)=2$，

因为 $\varphi(11)=10$，$5^2 \equiv 3$，$5^5 \equiv 45 \equiv 1 \pmod{11}$，所以 $\mathrm{ord}_{11}(5)=5$，所以 $5 \mid \mathrm{ord}_{121}(5)$，

因为 $\varphi(121)=121-11=110$，所以 $\mathrm{ord}_{121}(5) \mid 110$，

所以 $\mathrm{ord}_{121}(5)$ 可能为 5、10、55 或 110，

因为 $5^5 \equiv 100$，$5^{10} \equiv 78$，$5^{55} \equiv 1 \pmod{121}$，所以 $\mathrm{ord}_{121}(5)=55$，

所以 $\mathrm{ord}_{2904}(5)=[\mathrm{ord}_8(5), \mathrm{ord}_3(5), \mathrm{ord}_{121}(5)]=[2,2,55]=110$。

例 3.11 请计算模 23 的一个原根。

解：因为 $\varphi(23)=22$，　　所以 $\mathrm{ord}_{23}(a)$ 可能为 1、2、11、22，

因为 $2^2 \equiv 4$，$2^{11} \equiv 1 \pmod{23}$，　　所以 $\mathrm{ord}_{23}(2)=11$，

又因为 $\mathrm{ord}_{23}(-1)=2$，而 $(-1\times 2, 23)=(21,23)=1$，

所以 $\mathrm{ord}_{23}(-2)=\mathrm{ord}_{23}(21)=\mathrm{ord}_{23}(-1)\times\mathrm{ord}_{23}(2)=22$，即 21 为模 23 的一个原根。

3.2 原根

本节主要讨论原根的价值、存在性，以及计算技巧。

定理 3.3 若 $a, m, k \in \mathbf{Z}^+$，$(a,m)=1$，记 $n=\mathrm{ord}_m(a)$，$s=\mathrm{ord}_m(a^k)$，则

$$s = n/(k,n) \tag{3-1}$$

证明：因为 $(a^k)^s \equiv a^{ks} \equiv 1 \pmod m$，所以 $n \mid ks$，

所以 $n/(k,n) \mid ks/(k,n)$，所以 $n/(k,n) \mid s$，

所以 $(a^k)^{n/(k,n)}=(a^n)^{k/(k,n)} \equiv 1^{k/(k,n)} \equiv 1 \pmod m$，所以 $s \mid n/(k,n)$，

所以 $s=n/(k,n)$。证毕。

例 3.12 观察模 7 的一个缩系的元素与它们的指数，如表 3-4 所示。

表 3-4　模 7 的一个缩系的元素与它们的指数

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

(1) $\mathrm{ord}_7(2)=\mathrm{ord}_7(9)=\mathrm{ord}_7(3^2)=\mathrm{ord}_7(3)/(\mathrm{ord}_7(3),2)=6/(6,2)=3$;

(2) $\mathrm{ord}_7(4)=\mathrm{ord}_7(2^2)=\mathrm{ord}_7(2)/(\mathrm{ord}_7(2),2)=3/(3,2)=3$;

(3) $\mathrm{ord}_7(5)=\mathrm{ord}_7(3^5)=\mathrm{ord}_7(3)/(\mathrm{ord}_7(3),5)=6/(6,5)=6$。

【你应该知道的】

(1) 当$(k,n)=1$时，$s=n$，即$\mathrm{ord}_m(a^k)=\mathrm{ord}_m(a)$，因此模 m 的一个缩系中，与 a 指数相同的数有$\varphi(\mathrm{ord}_m(a))$个；

(2) 若 a 是模 m 的原根，则当$(k,\varphi(m))=1$时，a^k也是模 m 的原根；

(3) 如果模 m 存在原根，则不同的原根有 $\varphi(\varphi(m))$个。

例 3.13　观察模 7 的指数表可以看出：

因为 $\varphi(7)=6$ 的因子有 1、2、3、6，所以模 7 的指数可能为 1、2、3、6，

(1) 模 7 的指数为 6 的数字(原根)有 $\varphi(\varphi(7))=\varphi(6)=\varphi(2)\ \varphi(3)=2$ 个；

(2) 模 7 的指数为 3 的数字有 $\varphi(3)=2$ 个；

(3) 模 7 的指数为 2 的数字有 $\varphi(2)=1$ 个；

(4) 模 7 的指数为 1 的数字有 $\varphi(1)=1$ 个。

例 3.14　请计算模 23 的所有原根。

解：因为 -2 为模 23 的一个原根(见例 3.11)，

所以模 23 的原根有 $\varphi(\varphi(23))=\varphi(22)=\varphi(2)\times\varphi(11)=10$ 个，

所有原根可以表示为$(-2)^k \pmod{23}$，其中 $k=1、3、5、7、9、13、15、17、19、21$，即$(k,\varphi(23))=1$，

所以模 23 的所有原根有：$-2、-8、-9、-13、-6、-4、7、5、20、-12$。

即模 23 的所有原根有：5、7、10、11、14、15、17、19、20、21。

【你应该知道的】　利用原根生成缩系

根据定理 3.2(4)，可以利用模 m 一个原根，将模 m 的缩系中其余元素都表示出来，称为**可以用模 m 一个原根生成模 m 的缩系**，再利用定理 3.3，可以对应计算出模 m 的缩系的每个元素的指数。

例如，用模 7 的原根 3 生成模 7 的缩系，如表 3-5 所示。

表 3-5　以原根 3 生成模 7 的缩系

k	1	2	3	4	5	6
$a=3^k$	3	2	6	4	5	1

用模 7 的原根 5 生成模 7 的缩系，如表 3-6 所示。

表 3-6　以原根 5 生成模 7 的缩系

k	1	2	3	4	5	6
$a=5^k$	5	4	6	2	3	1

同样，可以分别用模 10 的原根 3 和 7 生成模 10 的缩系，如表 3-7 和表 3-8 所示。

表 3-7　以原根 3 生成模 10 的缩系

k	1	2	3	4
$a=3^k$	3	9	7	1

表 3-8　以原根 7 生成模 10 的缩系

k	1	2	3	4
$a=7^k$	7	9	3	1

据此可以对应计算出模 m 的缩系的每个元素的指数。

例如，用模 7 的原根 3 计算模 7 的缩系中每个元素的指数，如表 3-9 所示。

表 3-9　以原根 3 计算模 7 的缩系中每个元素的指数

k	6	2	1	4	5	3
$a=3^k$	1	2	3	4	5	6
$\mathrm{ord}_7(a)$	$6/(6,6)=1$	$6/(6,2)=3$	$6/(6,1)=6$	$6/(6,2)=3$	$6/(6,5)=6$	$6/(6,3)=2$

用模 7 的原根 5 计算模 7 的缩系中每个元素的指数，如表 3-10 所示。

表 3-10　以原根 5 计算模 7 的缩系中每个元素的指数

k	6	4	5	2	1	3
$a=5^k$	1	2	3	4	5	6
$\mathrm{ord}_7(a)$	$6/(6,6)=1$	$6/(6,2)=3$	$6/(6,5)=6$	$6/(6,2)=3$	$6/(6,1)=6$	$6/(6,3)=2$

同样，可以分别用模 10 的原根 3 和 7 生成模 10 的缩系中每个元素的指数，如表 3-11 所示。

表 3-11　以原根 3 和 7 生成模 10 的缩系中每个元素的指数

k	1	2	3	4
$a=3^k$	3	9	7	1
$\mathrm{ord}_{10}(a)$	$4/(4,1)=4$	$4/(4,2)=2$	$4/(4,3)=4$	$4/(4,4)=1$
$b=7^k$	7	9	3	1
$\mathrm{ord}_{10}(b)$	$4/(4,1)=4$	$4/(4,2)=2$	$4/(4,3)=4$	$4/(4,4)=1$

例 3.15　请计算模 23 的缩系的每个元素的指数。

解：因为 -2 为模 23 的一个原根（见例 3.11），$\varphi(23)=22$，

所以依次计算 -2 的幂得到：

$-2^2\equiv 4,-2^3\equiv 15,-2^4\equiv 16,-2^5\equiv 14,-2^6\equiv 18,-2^7\equiv 10,-2^8\equiv 3 \pmod{23}$，

$-2^9\equiv 17,-2^{10}\equiv 12,-2^{11}\equiv 22,-2^{12}\equiv 2,-2^{13}\equiv 19,-2^{14}\equiv 8,-2^{15}\equiv 7 \pmod{23}$，

$-2^{16}\equiv 9,-2^{17}\equiv 5,-2^{18}\equiv 13,-2^{19}\equiv 20,-2^{20}\equiv 6,-2^{21}\equiv 11,-2^{22}\equiv 1 \pmod{23}$，

所以模 23 的指数为 22 的有 $\varphi(22)=10$ 个：5、7、10、11、14、15、17、19、20、21。即分别为 $(-2)^k \pmod{23}$，其中，$(k,22)=22/22=1$（$k=1,3,5,7,9,13,15,17,19,21$）。

模 23 的指数为 11 的有 $\varphi(11)=10$ 个：2、3、4、6、8、9、12、13、16、18。即分别为 $(-2)^k \pmod{23}$，其中，$(k,22)=22/11=2$（$k=2,4,6,8,10,12,14,16,18,20$）。

模 23 的指数为 2 的有 $\varphi(2)=1$ 个：22。即分别为$(-2)^k \pmod{23}$，其中，$(k,22)=22/2=11(k=11)$，也就是$-1 \pmod{23}$。

模 23 的指数为 1 的有 $\varphi(1)=1$ 个：1。即分别为$(-2)^k \pmod{23}$，其中，$(k,22)=22/1=22(k=22)$。

例 3.16 请计算模 43 的缩系的每个元素的指数。

解：首先寻找模 43 的一个原根，从 2 开始计算。

因为 $\varphi(43)=42$，所以 $\mathrm{ord}_{43}(a)$可能为 1、2、3、6、7、14、21、42，

因为 $2^2\equiv 4, 2^3\equiv 8, 2^6\equiv 21, 2^7\equiv 42, 2^{14}\equiv 1 \pmod{43}$，所以 2 不是模 43 的原根。

因为 $3^2\equiv 9, 3^3\equiv 27, 3^6\equiv 41, 3^7\equiv 37, 3^{14}\equiv 36, 3^{21}\equiv 42 \pmod{43}$，

所以 3 是模 43 的原根。

接着依次计算 3 的幂，如表 3-12 所示。

表 3-12 3 的幂

k	$3^k \pmod{43}$	k	$3^k \pmod{43}$	k	$3^k \pmod{43}$
1	3	15	22	29	18
2	9	16	23	30	11
3	27	17	26	31	33
4	38	18	35	32	13
5	28	19	19	33	39
6	41	20	14	34	31
7	37	21	42	35	7
8	25	22	40	36	21
9	32	23	34	37	20
10	10	24	16	38	17
11	30	25	5	39	8
12	4	26	15	40	24
13	12	27	2	41	29
14	36	28	6	42	1

最后根据 k 的取值可以得到表 3-13。

表 3-13 根据 k 值计算 a

$\mathrm{ord}_{43}(a)$	a 的个数	a
1	$\varphi(1)=1$	1
2	$\varphi(2)=1$	42
3	$\varphi(3)=2$	6,36
6	$\varphi(6)=2$	7,37
7	$\varphi(7)=6$	4,11,16,21,35,41
14	$\varphi(14)=6$	2,8,22,27,32,39
21	$\varphi(21)=12$	9,10,13,14,15,17,23,24,25,31,38,40
42	$\varphi(42)=12$	3,5,12,18,19,20,26,28,29,30,33,34

整理一下，可以形成模 43 的指数表如表 3-14 所示。

表 3-14　模 43 指数表

a	$\mathrm{ord}_{43}(a)$	a	$\mathrm{ord}_{43}(a)$	a	$\mathrm{ord}_{43}(a)$
1	1	15	21	29	42
2	14	16	7	30	42
3	42	17	21	31	21
4	7	18	42	32	14
5	42	19	42	33	42
6	3	20	42	34	42
7	6	21	7	35	7
8	14	22	14	36	3
9	21	23	21	37	6
10	21	24	21	38	21
11	7	25	21	39	14
12	42	26	42	40	21
13	21	27	14	41	7
14	21	28	42	42	2

定理 3.4　原根存在条件

模 m 有原根的存在的充要条件是 $m=2,4,p^{\alpha}$ 或 $2p^{\alpha}$，其中，p 是奇素数，整数 $\alpha\geqslant 1$。

我们重点关注模 m 是奇素数时原根的计算技巧。

定理 3.5　设 p 是奇素数，$p-1=\prod_{k=1}^{s}p_k^{q_k}$，$p_k$ 为不同素数，若 $(a,p)=1$，a 是模 p 的原根的充要条件是：

$$a^{\frac{p-1}{p_i}}\not\equiv 1(\bmod p),\quad i=1,2,\cdots,k \tag{3-2}$$

证明：($\Rightarrow$)若 a 是模 p 的一个原根，p 是奇素数，则 $\mathrm{ord}_p(a)=\varphi(p)=p-1$，

因为 $0<\varphi(p)/p_i<\varphi(p)$，$p_i$ 为不同素数，$i=1,2,\cdots,k$，

所以根据定义 3.1，$a^{\frac{p-1}{p_i}}\not\equiv 1(\bmod p)$。

($\Leftarrow$)若当 $a^{\frac{p-1}{p_i}}\not\equiv 1(\bmod p)$，$i=1,2,\cdots,k$ 成立时，$\mathrm{ord}_p(a)<\varphi(p)=p-1$，

因为根据定理 3.1，$\mathrm{ord}_p(a)\mid\varphi(p)$，设 $e=\mathrm{ord}_p(a)$，

所以存在一个素数 p_i，使得 $p_i\mid(p-1)/e$，即 $(p-1)/e=q\times p_i$，即 $(p-1)/p_i=qe$，

所以存在 $a^{\frac{p-1}{p_i}}\equiv a^{qe}\equiv 1(\bmod p)$，与题设矛盾，

所以 $\mathrm{ord}_p(a)=\varphi(p)$，即 a 是模 p 的一个原根。

证毕。

例 3.17　请计算模 113 的一个原根。

解：因为 $\varphi(113)=112=2^4*7$，所以只需计算 a^{16}，$a^{56}(\bmod 113)$，

因为 $2^{16}\equiv 109$，$2^{56}\equiv 1\ (\bmod 113)$，所以 2 不是模 113 的原根，

因为 $3^{16}\equiv 49$，$3^{56}\equiv -1\ (\bmod 113)$，所以 3 是模 113 的原根。

例 3.18　请生成模 113 的缩系的所有元素的指数表。

解：根据例 3.17，3 是模 113 的原根，所以依次计算 3 的幂，如表 3-15 所示。

据此可以形成模 113 的指数表，如表 3-16 所示。

表 3-15　3 的幂

k	$3^k \pmod{113}$	k	$3^k \pmod{113}$	k	$3^k \pmod{113}$	k	$3^k \pmod{113}$	k	$3^k \pmod{113}$
1	3	24	4	47	43	70	95	93	89
2	9	25	12	48	16	71	59	94	41
3	27	26	36	49	48	72	64	95	10
4	81	27	108	50	31	73	79	96	30
5	17	28	98	51	93	74	11	97	90
6	51	29	68	52	53	75	33	98	44
7	40	30	91	53	46	76	99	99	19
8	7	31	47	54	25	77	71	100	57
9	21	32	28	55	75	78	100	101	58
10	63	33	84	56	112	79	74	102	61
11	76	34	26	57	110	80	109	103	70
12	2	35	78	58	104	81	101	104	97
13	6	36	8	59	86	82	77	105	65
14	18	37	24	60	32	83	5	106	82
15	54	38	72	61	96	84	15	107	20
16	49	39	103	62	62	85	45	108	60
17	34	40	83	63	73	86	22	109	67
18	102	41	23	64	106	87	66	110	88
19	80	42	69	65	92	88	85	111	38
20	14	43	94	66	50	89	29	112	1
21	42	44	56	67	37	90	87		
22	13	45	55	68	111	91	35		
23	39	46	52	69	107	92	105		

表 3-16　模 113 指数表

a	$\mathrm{ord}_{113}(a)$	a	$\mathrm{ord}_{113}(a)$	a	$\mathrm{ord}_{113}(a)$	a	$\mathrm{ord}_{113}(a)$	a	$\mathrm{ord}_{113}(a)$
1	1	24	112	47	112	70	112	93	112
2	28	25	56	48	16	71	16	94	112
3	112	26	56	49	7	72	56	95	8
4	14	27	112	50	56	73	16	96	112
5	112	28	7	51	56	74	112	97	14
6	112	29	112	52	56	75	112	98	4
7	14	30	7	53	28	76	112	99	28
8	28	31	56	54	112	77	56	100	56
9	56	32	28	55	112	78	16	101	112
10	112	33	112	56	28	79	112	102	56
11	56	34	112	57	28	80	112	103	112
12	112	35	16	58	112	81	28	104	56
13	56	36	56	59	112	82	56	105	28
14	28	37	112	60	28	83	14	106	7
15	4	38	112	61	56	84	112	107	112
16	7	39	112	62	56	85	14	108	112
17	112	40	16	63	56	86	112	109	7
18	8	41	56	64	14	87	56	110	112
19	112	42	16	65	16	88	56	111	28
20	112	43	112	66	112	89	112	112	2
21	112	44	8	67	112	90	112		
22	56	45	112	68	112	91	56		
23	112	46	112	69	8	92	112		

3.3 离散对数方程

定义 3.3 离散对数

设整数 $m>1$，g 是模 m 的一个原根，$(a,m)=1$，则存在唯一整数 r，$1\leqslant r\leqslant\varphi(m)$，使

$$g^r \equiv a \pmod{m} \tag{3-3}$$

则 r 叫作以 g 为底的 a 对模 m 的一个离散对数，记为 $r=\mathrm{ind}_g a$。

如当 $m=7$，$g=3$ 时，有如表 3-17 所示数据。

表 3-17 $m=7$，$g=3$ 时数据表

k	1	2	3	4	5	6
$a=g^k$	3	2	6	4	5	1

即可以形成以 3 为底的模 7 的离散对数表，如表 3-18 所示。

表 3-18 以 3 为底的模 7 离散对数表

a	1	2	3	4	5	6
$\mathrm{ind}_g a$	0	2	1	4	5	3

【请你注意】

(1) $\mathrm{ind}_g a$ 也称为指标，有的也简单记为 $\mathrm{ind}a$，或者直接记为 $\log_g a$；

(2) $\mathrm{ind}_g a$ 与对数具有相似的性质，如

当 $\mathrm{ind}_g a=1$ 时，$a=g$；

$g^{\mathrm{ind}_g a}\equiv a \pmod{m}$；

$\mathrm{ind}_g a+\mathrm{ind}_g b=\mathrm{ind}_g(ab) \pmod{\varphi(m)}$等；

(3) 使得 $g^x\equiv a \pmod{m}$成立的所有整数 x 可表示为 $x\equiv\mathrm{ind}_g a \pmod{\varphi(m)}$。

例 3.19 请写出模 43 的离散对数表。

解：根据例 3.16，3 是模 43 的一个原根，根据 3 的幂，写出以 3 为底模 43 的离散对数表，如表 3-19 所示。

表 3-19 以 3 为底模 43 的离散对数表

十位＼个位	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0		0	27	1	12	25	28	35	39	2
1	10	30	13	32	20	26	24	38	29	19
2	37	36	15	16	40	8	17	3	5	41
3	11	34	9	31	23	18	14	7	4	33
4	22	6	21							

例 3.20 请计算模 43 的 $\mathrm{ind}_3 28$，$\mathrm{ind}_3 37$。

解：根据例 3.19，查找十位数 2 所在的行和个位数 8 所在的列，交叉位置为 5，因此

$\text{ind}_3 28=5$；查找十位数 3 所在的行和个位数 7 所在的列，交叉位置为 7，因此 $\text{ind}_3 37=7$。

例 3.21 解方程 $x^5\equiv 3 \pmod 7$。

解：（法一）：$\text{ind}_3 x^5\equiv \text{ind}_3 3 \pmod{\varphi(7)}$，即 $5\text{ind}_3 x\equiv 1 \pmod 6$，

因为 $6=5\times 1+1$，所以 $5^{-1}\pmod 6=-1$，所以 $\text{ind}_3 x\equiv -1\equiv 5 \pmod 6$，

因为以 3 为底模 7 的离散对数表如表 3-20 所示。

表 3-20 以 3 为底模 7 的离散对数表

a	1	2	3	4	5	6
$\text{ind}_g a$	0	2	1	4	5	3

所以 $x\equiv 5 \pmod 7$。

当然，也可以利用以 5 为底模 7 的离散对数表，如表 3-21 所示。

表 3-21 以 5 为底模 7 的离散对数表

a	1	2	3	4	5	6
$\text{ind}_g a$	0	4	5	2	1	3

（法二）：$\text{ind}_5 x^5\equiv \text{ind}_5 3 \pmod{\varphi(7)}$，即 $5\ \text{ind}_5 x\equiv 5 \pmod 6$，

所以 $\text{ind}_5 x\equiv 1 \pmod 6$，所以 $x\equiv 5 \pmod 7$。

例 3.22 解方程 $x^{22}\equiv 23 \pmod{43}$。

解：利用例 3.19 的离散对数表有 $22\ \text{ind}_3 x\equiv \text{ind}_3 23\equiv 16 \pmod{42}$，

所以化简得 $11\ \text{ind}_3 x\equiv 8 \pmod{21}$，所以 $\text{ind}_3 x\equiv 8\times 2\equiv 16 \pmod{21}$，

所以 $\text{ind}_3 x\equiv 16,37 \pmod{42}$，所以 $x\equiv 20,23 \pmod{43}$。其实就是 $x\equiv\pm 20 \pmod{43}$。

例 3.23 解方程 $6\times 3^x\equiv 5 \pmod 7$。

解：（法一）：$3^x\equiv 5\times(-1)\equiv 2 \pmod 7$，所以 $x\ \text{ind}_3 3\equiv \text{ind}_3 2 \pmod 6$，所以 $x\equiv 2 \pmod 6$。

（法二）：$\text{ind}_3 6+\ \text{ind}_3 3^x\equiv \text{ind}_3 5 \pmod 6$，所以 $3+x\equiv 5 \pmod 6$，所以 $x\equiv 2 \pmod 6$。

【思考】

k 为整数，求解 $x^k\equiv 1 \pmod{11}$。

提示：$\text{ind}_{11} x$ 是 $\varphi(11)$ 的因子，因此 $\text{ind}_{11}(x)$ 可能为 1、2、5、10，但是 k 的取值不只是 1、2、5、10，如 $x\equiv 1 \pmod{11}$ 一定是 $x^k\equiv 1 \pmod{11}$ 的解，此时 k 可以为任何整数。

例 3.24 解方程 $x^5\equiv 3 \pmod{301}$。

解：$x^5\equiv 3(\text{mod } 301) \quad \Leftrightarrow \quad \begin{cases} x^5\equiv 3(\text{mod } 7) \\ x^5\equiv 3(\text{mod } 43) \end{cases}$

所以根据例 3.21，$x\equiv 5 \pmod 7$，

利用例 3.19 的离散对数表有 $5\ \text{ind}_{113} x\equiv \text{ind}_{113} 3\equiv 1 \pmod{42}$，

有 $\text{ind}_{113} x\equiv 17 \pmod{42}$，$x\equiv 3^{17}(\text{mod } 43)\equiv 26$，

所以根据孙子定理 $x\equiv 5\times 43\times 1+26\times 7\times(-6) \pmod{301}\equiv 26$。

例 3.25 解方程 $5^x\equiv 3 \pmod{301}$。

解：$5^x\equiv 3(\text{mod } 301) \quad \Leftrightarrow \quad \begin{cases} 5^x\equiv 3(\text{mod } 7) \\ 5^x\equiv 3(\text{mod } 43) \end{cases}$，

以 3 为底模 7 的离散对数表如表 3-22 所示。

表 3-22　以 3 为底模 7 的离散对数表

a	1	2	3	4	5	6
$\mathrm{ind}_g a$	0	2	1	4	5	3

所以 $x\mathrm{ind}_3 5\equiv\mathrm{ind}_3 3\pmod 6$，所以 $5x\equiv 1\pmod 6$，所以 $x\equiv 5\pmod 6$，

利用例 3.19 的离散对数表有 $x\ \mathrm{ind}_3 5\equiv \mathrm{ind}_3 3\equiv 1\pmod{42}$，

所以 $25x\equiv 1\pmod{42}$，$x\equiv -5\equiv 37\pmod{42}$，

因为 $x\equiv 5\pmod 6\equiv 5,11,17,23,29,35,41\pmod{42}$，

所以此方程无解。

例 3.26　解方程 $5^x\equiv 12\pmod{301}$。

解：$5^x\equiv 12(\mathrm{mod}\ 301)\quad\Leftrightarrow\quad\begin{cases}5^x\equiv 12\equiv 5(\mathrm{mod}\ 7)\\5^x\equiv 12(\mathrm{mod}\ 43)\end{cases}$，

所以 $x\equiv 1\pmod 6$，

所以 $x\ \mathrm{ind}_3 5\equiv \mathrm{ind}_3 12\pmod{42}$，所以 $25x\equiv 13\pmod{42}$，所以 $x\equiv 19\pmod{42}$，

因为 $x\equiv 1\pmod 6\equiv 1,7,13,19,25,31,37\pmod{42}$，

所以 $x\equiv 19\pmod{42}$。

【进一步的知识】　离散对数密码算法

现有的非对称密码算法的安全性大都是依赖数论中的一些难题：处理过程计算上的不可逆性(陷门)。

RSA 公钥密码算法依赖的就是因子分解难题：对于大整数，已知 p、q，就可以很直接地计算出 $n=p\times q$，但如果已知的是 n，分解出 n 的因子，计算是非常耗时的，并没有快速有效的算法。

离散对数问题也是一个数学难题：已知模 n 的原根 g，给定整数 r，计算出 $a\equiv g^r(\mathrm{mod}\ n)$很简单，但若已知 n、g、a，计算出整数 r 就非常困难。

ElGamal 公钥密码算法就是依赖于上述离散对数难题，具体过程描述如下。

1. 生成公钥和私钥

(1) 选择大整数 p 和 p 的一个原根 g；

(2) 随机选取整数 a，$1<a<p-1$，计算 $b\equiv g^a(\mathrm{mod}\ p)$；

(3) (p,g,b)为公钥，a 为私钥。

2. ElGamal 公钥密码算法进行加密/解密

(1) 加密：将信息表示为整数 m，$0\leqslant m\leqslant p-1$，随机选择整数 k，$1\leqslant k\leqslant p-1$，计算出 $c_1\equiv g^k(\mathrm{mod}\ p)$，$c_2\equiv m\times b^k(\mathrm{mod}\ p)$，加密后的密文为 $c=(c_1,c_2)$。

(2) 解密：解密后的明文为 $m\equiv c_2\times(c_1^a)^{-1}(\mathrm{mod}\ p)$。

证明：因为 $c_2\times(c_1^a)^{-1}(\mathrm{mod}\ p)\equiv mb^k(g^{ka})^{-1}\equiv mg^{ak}(g^{ka})^{-1}\equiv m(\mathrm{mod}\ p)$，

所以解密变换能正确从密文恢复出相应的明文，证毕。

例 3.27　选择素数 p 为 4519 和其原根 $g=3$，私钥 $a=111$，请计算：

(1) 公钥 b;

(2) 选择随机整数 $k=891$,将字母“A”加密后发送;

(3) 对收到的密文进行解密验证。

解:(1) $b\equiv g^a \pmod p \equiv 638$;

(2) 要加密字母“A”,即明文 $m=65$,则 $c_1\equiv g^k \pmod p \equiv 2577$,

$c_2\equiv m\times b^k \equiv 65\times 638^{891} \equiv 65\times 3274\equiv 417 \pmod p$,

所以,密文为(2577,417);

(3) 解密:$m\equiv c_2\times (c_1^a)^{-1}\equiv 417\times 2577^{-111}\equiv 417\times 3274^{-1}\equiv 417\times 1539\equiv 65 \pmod{4519}$;

密文被解密成字母“A”。

Diffie-Hellman 密钥协商机制也依赖离散对数问题,实现发送方 A 和接收方 B 随机产生一个只有两人知道的共同的密钥。它是 W. Diffie 和 M. E. Hellman 在 1976 年提出的一个奇妙的密钥交换的协议,通信双方可以使用这个机制确定对称密钥,然后使用这个密钥进行加密和解密。其具体过程描述如下。

1. 初始化

(1) 选择大素数 p,计算其一个原根 g;

(2) A 产生一个随机数 x_A,$1\leqslant x_A<p$,作为私钥;计算公钥 $y_A\equiv g^{x_A} \pmod p$;

(3) B 产生一个随机数 x_B,$1\leqslant x_B<p$,作为私钥;计算公钥 $y_B\equiv g^{x_B} \pmod p$。

2. 计算共享密钥

(1) A 利用自己的私钥 x_A和 B 的公钥 y_B,计算加密密钥 $K_A\equiv y_B^{x_A}\equiv g^{x_A\times x_B} \pmod p$;

(2) B 利用自己的私钥 x_B和 A 的公钥 y_A,计算加密密钥 $K_B\equiv y_A^{x_B}\equiv g^{x_A\times x_B} \pmod p$。

所以 A 和 B 各自生成的密钥 $K_A\equiv K_B$,可以用作对称加密密钥。第三方只能获取 p,g,$g^{x_A} \pmod p$,$g^{x_B} \pmod p$,无法求得 $g^{x_A\times x_B} \pmod p$。

例 3.28 选择素数 p 为 4519 和其原根 $g=3$,A 选择私钥 $x_A=36$,B 选择私钥 $x_B=58$,请利用仿射密码($c\equiv Km \pmod p$和 $m\equiv K^{-1}c \pmod p$)和指数密码($c\equiv m^K \pmod p$和 $m\equiv c^{K^{-1} \pmod{p-1}} \pmod p$)实现字母“A”的传递。

解:(1) A 计算公钥:$y_A\equiv g^{x_A} \pmod p \equiv 3^{36} \pmod{4519} \equiv 3975$,

B 计算公钥:$y_B\equiv g^{x_B} \pmod p \equiv 3^{58} \pmod{4519}\equiv 1163$。

(2) A 计算加密密钥:$K_A\equiv y_B^{x_A} \pmod p \equiv 1163^{36} \pmod{4519} \equiv 1627$,

B 计算解密密钥:$K_B\equiv y_A^{x_B} \pmod p \equiv 3975^{58} \pmod{4519}\equiv 1627$。

(3) A 利用 K_A使用仿射密码加密“A”:

即明文 $m=65$,则 $c\equiv Km \pmod p \equiv 1627\times 65 \pmod{4519} \equiv 1818$。

A 将“1818”发送给 B;

B 利用 K_B使用仿射密码解密“1818”:

因为 $4519=1627\times 3-362$,$1627=362\times 4+179$,$362=179\times 2+4$,$179=4\times 45-1$,

所以 $1=4\times 45-179=(362-179\times 2)\times 45-179=362\times 45-179\times 91$

$=362\times 45-(1627-362\times 4)\times 91=362\times 409-1627\times 91$

$=(1627\times 3-4519)\times 409-1627\times 91=1627\times 1136-4519\times 409$,

所以 $K^{-1}(\mathrm{mod}\ p)\equiv 1627^{-1}(\mathrm{mod}\ 4519)\equiv 1136$，

则 $m\equiv K^{-1}c(\mathrm{mod}\ p)\equiv 1136\times 1818\ (\mathrm{mod}\ 4519)\equiv 65$；

B恢复出明文“A”。

(4) A利用 K_A使用指数密码加密“A”：

所以 $c\equiv m^K(\mathrm{mod}\ p)\equiv 65^{1627}(\mathrm{mod}\ 4519)\equiv 2836$，

所以A将“2836”发送给B。

B利用 K_B使用指数密码解密“2836”：

因为 $4518=1627\times 3-363$，$1627=363\times 4+175$，$363=175\times 2+13$，

$175=13\times 13+6$，$13=6\times 2+1$，

所以 $1=13-6\times 2=13-(175-13\times 13)\times 2=13\times 27-175\times 2$

$=(363-175\times 2)\times 27-175\times 2$

$=363\times 27-175\times 56=363\times 27-(1627-363\times 4)\times 56=363\times 251-1627\times 56$

$=(1627\times 3-4518)\times 251-1627\times 56=1627\times 697-4518\times 251$，

所以 $K^{-1}(\mathrm{mod}\ p-1)\equiv 1627^{-1}(\mathrm{mod}\ 4518)\equiv 697$，

所以 $m\equiv c^{K^{-1}(\mathrm{mod}\ p-1)}(\mathrm{mod}\ p)\equiv 2836^{697}(\mathrm{mod}\ 4519)\equiv 65$，

B恢复出明文“A”。

小结

本章以解离散对数方程为目的，研究了原根与指数，主要内容可以归纳为以下4个要点。

1. 指数与原根

1) 指数

(1) $(a,m)=1$，使 $a^k\equiv 1\ (\mathrm{mod}\ m)$成立的最小正整数 k，写作 $\mathrm{ord}_m(a)$或$\delta_m(a)$；

(2) 指数整除欧拉函数；

(3) 等指数：模 m 同余、互逆的数的指数相同。

2) 原根

(1) 模 m 的缩系中指数与欧拉函数相等的数；

(2) 模 m 有原根的必要条件是 $m=2,4,p^\alpha$ 或 $2\ p^\alpha$，其中，p 是奇素数，$\alpha\geqslant 1$。

2. 指数与原根的计算技巧

1) 计算指数的技巧

(1) 幂指数从小到大取欧拉函数的因数试算，直到幂等于1；

(2) $(m,n)=1,(a,mn)=1$，则 $\mathrm{ord}_{mn}(a)=[\mathrm{ord}_m(a),\mathrm{ord}_n(a)]$；

(3) $(ab,m)=1,(\mathrm{ord}_m(a),\mathrm{ord}_m(b))=1$，则 $\mathrm{ord}_m(ab)=\mathrm{ord}_m(a)\ \mathrm{ord}_m(b)$；

(4) $(a,m)=1,k\in\mathbf{Z}^+$，则 $\mathrm{ord}_m(a^k)=\mathrm{ord}_m(a)/(k,\mathrm{ord}_m(a))$。

2) 计算原根的技巧

p 是奇素数，$p-1=\prod_{k=1}^{s}p_k^{a_k}$，若$(a,p)=1$，

a 是模 p 的原根 $\Leftrightarrow a^{\frac{p-1}{p_k}} \not\equiv 1 \pmod{p}$，$k=1,2,\cdots,s$。

3. 指数与原根的计算价值

(1) 指数的价值：幂指数化简。

(2) 原根 g 的价值：

① 生成元：生成缩系的所有元素，$\{g^k \mid k \in \mathbf{Z}\}$。

② k 与 g^k 形成一一映射。

③ 可以根据幂指数 k 对模 m 的缩系元素分类。

④ k 遍历 $\varphi(m)$ 的缩系，g^k 遍历模 m 的原根。

⑤ 可以计算出模 m 的缩系的所有元素的指数。

4. 利用离散对数表解高阶指数方程

(1) 离散对数：$g^r \equiv a \pmod{m}$，$r=\mathrm{ind}_g a$，要求 g 是原根和 $(a,m)>1$。

(2) 类似对数解指数方程：

① 原根为底，“≡”左右取离散对数，模变欧拉函数。

② 未知数 x 位于底数，解的模为 m；x 位于指数，解的模为 $\varphi(m)$。

作业

1. 请计算下面的指数：

(1) $\mathrm{ord}_{11}(5)$　　(2) $\mathrm{ord}_{77}(5)$　　(3) $\mathrm{ord}_{121}(5)$

(4) $\mathrm{ord}_{36}(5)$　　(5) $\mathrm{ord}_{36}(25)$　　(6) $\mathrm{ord}_{36}(55)$

2. 请写出模 47 的所有原根。

3. 请找到模 101 的一个原根，并写出缩系中指数为 5 的所有元。

4. 请建立模 17 的离散对数表，并求解方程 $7x^6 \equiv 11 \pmod{17}$。

5. 利用模 43 的离散对数表求解：

(1) $x^6 \equiv 11 \pmod{43}$　　(2) $6^x \equiv 11 \pmod{43}$

(3) $5x^6 \equiv 11 \pmod{43}$　　(4) $6^{5x} \equiv 11 \pmod{43}$

6. k 为整数，求解 $x^k \equiv 1 \pmod{11}$。

7. 写出所有整数 m，使得关于 x 的同余方程 $mx^5 \equiv 7 \pmod{29}$ 有解。

8. 设使用 ElGamal 公钥密码进行消息传输，私钥为 $(641,3,15)$，请问：

(1) 公钥为多少？

(2) 选择随机整数，$k=123$，字母“A”被转换为的密文是什么？

(3) 你能通过解密过程验证第(2)步中加密计算的正确性吗？

9. 设 Diffie-Hellman 密钥交换协议中，公用素数 $p=17$，原根 g 为 3，若用户 A 的公钥 $y_A=9$，则 A 的私钥 x_A 为多少？若 B 的公钥 $y_B=9$，则加密密钥 K_A 和 K_B 为多少？

10. 请设计实现建立某个数字的离散对数表的程序，完成：

(1) 写出该程序的关键步骤(功能模块)。

(2) 求出 967 的原根中最小的一个 g，建立其离散对数表，根据该表，计算出 $\mathrm{ind}g(15)$，

求解 $x^6 \equiv 11 \pmod{967}$。

(3) 977 有原根吗,987 呢?

11. Hash 函数(散列函数)可将任意长度的消息映射成固定长度的消息。Chaum、Heijst 和 Pfitzmann 在 1992 年提出利用离散对数可以构造 Hash 函数,构造的具体方法如下。

设 p 是一个大素数,$q=(p-1)/2$ 也是一个素数,a 和 b 为模 p 的两个原根,定义 Hash 函数为 $h(x_1,x_2)=a^{x_1}\times b^{x_2} \pmod{p}$。

设 x_1 和 x_2 是两个不同的消息,如果 $h(x_1)=h(x_2)$,则称 x_1 和 x_2 是一个碰撞。

可以证明前述 Hash 函数是抗碰撞的,这是因为若 (x_1,x_2) 和 (x_3,x_4) 是一对碰撞消息(即 $(x_1,x_2)\neq(x_3,x_4)$ 时 $h(x_1,x_2)=h(x_3,x_4)$),可以计算出 $\mathrm{ind}_a b$,与“离散对数的计算是一个难题”矛盾。

(1) 你能计算出 $\mathrm{ind}_a b$ 吗?

(2) 为什么要求 $(p-1)/2$ 也是一个素数?

12. 定点攻击的实现在 RSA 公钥密码机制中,设 B 的公钥为 (n,e),私钥为 (n,d)。A 将明文 M 用 B 的公钥加密为密文 C 后,发送给 B,但中途被 C 截获,C 截获后不知 d,故无法将 C 直接还原为 M,就反复计算 C 的 e 次幂,可以将 C 还原为明文 M,实现攻击,请问:

(1) 实现攻击的数学原理是什么(C 如何可以计算出原来的明文 M)?

(2) 可以对哪些参数采取限制条件减少攻击成功的可能性?