第3章

有限域与群

只含有限个元素的域称为有限域(Finite Field),也称为伽罗瓦域(Galois Field),由伽罗瓦(Évariste Galois)于18世纪30年代研究代数方程根式求解问题时引出。群是一种只含有单个运算的比较简单的代数系统,也是用于建立其他代数系统的一种基本结构。

这一章将学习域和群的相关知识,包括域的阶和特征,群的基本概念、元素的阶、循环群与生成元等,并结合密码学中的相关算法与协议,了解域和群理论在网络空间安全中的应用。

3.1 域的特征与费马小定理

在第2章,已经了解了环和域的基本概念,与元素个数无限的数域相比,有限域有着很多重要的性质,例如有限性、可逆性、封闭性、安全性、构造简单且高效等,在密码学中具有特别的意义。

定义 3.1.1 设 F 是一个非空集合,且是一个域,若 F 只包含有限个元素,则称 F 为**有限域**,或者**伽罗瓦域**,其元素的个数 q 称为有限域的**阶**,该域可记作 $\mathrm{GF}(q)$或者 F_q,表示 q 阶有限域。

在模 p 剩余类域 $\mathbf{Z}_p$、有理数域 $\mathbf{Q}$、实数域 $\mathbf{R}$ 中,可以观察到如表3-1所示的现象。

表 3-1 案例

域	现 象
$\mathbf{Z}_2$	$2\bar{1}=\bar{1}+\bar{1}=\bar{2}=\bar{0}$
$\mathbf{Z}_3$	$3\bar{1}=\bar{1}+\bar{1}+\bar{1}=\bar{3}=\bar{0}$
$\mathbf{Z}_p$	$p\bar{1}=\underbrace{\bar{1}+\bar{1}+\bar{1}+\cdots+\bar{1}}_{p}=\bar{p}=\bar{0}$
$\mathbf{Q}$	$n1=\underbrace{1+1+\cdots+1}_{n}\neq 0,\forall n\in N^*$
$\mathbf{R}$	$n1=\underbrace{1+1+\cdots+1}_{n}\neq 0,\forall n\in N^*$

从上面的例子可以观察到，在域 F 中，其单位元 e 的正整数倍是否等于零元，有以下两种情形。

(1) 存在一个素数 p，使得 $pe=0$，并设 p 是使得 $pe=0$ 成立的最小正整数。

(2) 对任意正整数 n，都有 $ne\neq 0$。

于是，下面的结论成立。

定理 3.1.1 在域 F 中，要么对于任意正整数 n，都有 $ne\neq 0$，要么存在一个素数 p，使得 $pe=0$，且 $le\neq 0$，$0<l<p$。

证明 对于情形(1)，假设 p 不是素数，则

$$p=p_1p_2,\quad 1<p_1<p,\quad 1<p_2<p$$

因为 $1<p_1<p$，$1<p_2<p$，从而有 $p_1e\neq 0$，$p_2e\neq 0$。

将 p_1e 和 p_2e 相乘，得

$$(p_1e)(p_2e)=p_1(ep_2e)=p_1[p_2(ee)]=p_1p_2e=pe=0$$

对于元素 p_1e，找到了一个非零元 p_2e，两者相乘得零元，则元素 p_1e 是零因子。根据结论“环中零因子不是可逆元”，从而元素 p_1e 不是可逆元。此结论与域的定义“非零元都是可逆元”矛盾，因此，假设不成立，p 一定是素数。

根据定理 3.1.1，引出域的特征(Characteristic)。

定义 3.1.2 在域 F 中，如果对于任意正整数 n，都有 $ne\neq 0$，那么称域 F 的**特征为 0**，如果存在一个素数 p，使得 $pe=0$，且 $le\neq 0$，$0<l<p$，那么称域 F 的**特征为 p**，可记作 $\mathrm{char}\,F$。

例 3.1 任一数域和模 p 剩余类域 $\mathbf{Z}_p$ 的特征分别是多少？

解 根据定义 3.1.2，分别是 0 和素数 p。

根据定义 3.1.2，在域 F 中，若特征为素数 p，则 $pe=0$。进一步思考，此结论对于 F 中任一元素 a 是否都成立？任一元素 a 的 p 倍，即任一元素 a 经过 p 次相加，记为 pa，是否等于 0 元？

通过分析，可以得出如下结论。

性质 3.1.1 设域 F 的特征为素数 p，对于域中任一元素 a，有 $pa=0$，$\forall a\in F$。

证明 根据已知条件，有

$$pa=p(ea)=(pe)a=0a=0$$

其中，e 为域 F 的单位元。

观察表 3-2 中模 p 剩余类域 $\mathbf{Z}_p$ 的案例，可以进一步探讨和分析其中蕴含的规律。

表 3-2 案例

域	现 象
$\mathbf{Z}_2$	$(a+b)^2=a^2+2ab+b^2=a^2+b^2$，$\forall a,b\in\mathbf{Z}_2$
$\mathbf{Z}_3$	$(a+b)^3=a^3+3a^2b+3ab^2+b^3=a^3+b^3$，$\forall a,b\in\mathbf{Z}_3$
$\mathbf{Z}_5$	$(a+b)^5=a^5+5a^4b+10a^3b^2+10a^2b^3+5ab^4+b^5=a^5+b^5$，$\forall a,b\in\mathbf{Z}_5$

通过上面的案例，发现模 p 剩余类域 $\mathbf{Z}_p$ 中，$(a+b)^p=a^p+b^p$，即有如下结论。

性质 3.1.2 设域 F 的特征为素数 p，对于域中任一元素 a 和 b，有

$$(a+b)^p=a^p+b^p,\quad \forall a,b\in F$$

证明* 域 F 与实数域类似，具有同样的运算法则，因此，在域 F 中应用二项式定理，有

$$(a+b)^p = a^p + C_p^1 a^{p-1}b + \cdots + C_p^k a^{p-k}b^k + \cdots + C_p^{p-1}ab^{p-1} + b^p$$

上式中，如果组合数的通项 C_p^k 能够被 p 整除，即 $C_p^k = qp$，$q \in N^*$，根据性质 3.1.1，则 $C_p^k a^{p-k}b^k = pqa^{p-k}b^k = p(qa^{p-k}b^k) = 0$，$1 \leqslant k < p$，即中间项全部为 0，则有 $(a+b)^p = a^p + b^p$，性质 3.1.2 成立。

现在的问题转变成 p 是否整除 C_p^k，即 $p \mid C_p^k$？

把组合数 C_p^k 展开，有

$$C_p^k = \frac{p(p-1)(p-2)\cdots(p-k+1)}{k!}, \quad 1 \leqslant k < p$$

进一步分析，在上述组合数 C_p^k 计算公式中，已经包含变量 p，如果要 p 整除 C_p^k，根据整除的定义，只要 $\frac{(p-1)(p-2)\cdots(p-k+1)}{k!}$ 为整数即可。

根据已知条件 $1 \leqslant k < p$，则 $p \nmid k$。根据素数的性质，对于任意整数 a，要么整除 $p \mid a$，要么互素 $(p,a)=1$，有 $(p,k)=1$。

根据互素的性质 2.3.3.3 的推广，若 $(a_i, c)=1$，$i=1,2,\cdots,n$，则 $(a_1 a_2 \cdots a_n, c)=1$。因为 $(p,1)=1$，$(p,2)=1$，$\cdots$，$(p,p-1)=1$，有 $(p,k!)=1$。同时，由组合数 C_p^k 展开公式，有 $k! \mid p(p-1)(p-2)\cdots(p-k+1)$，再根据互素的性质 2.3.3.1，可以得到 $k! \mid (p-1)(p-2)\cdots(p-k+1)$，即 $\frac{(p-1)(p-2)\cdots(p-k+1)}{k!}$ 为整数，则 $p \mid C_p^k$ 得证。

性质 3.1.2 可进一步推广为：设域 F 的特征为素数 p，对于域中任一元素 a_i，有

$$(a_1 + a_2 + \cdots + a_i + \cdots + a_n)^p = a_1^p + a_2^p + \cdots + a_i^p + \cdots + a_n^p, \quad \forall a_i \in F$$

例 3.2 79^{17} 模 17 同余于多少？

解 17 是素数，于是域 $\mathbf{Z}_{17}$ 的特征为 17，从而在域 $\mathbf{Z}_{17}$ 中有

$$\overline{79^{17}} = \overline{79}^{17} = (\underbrace{\bar{1}+\bar{1}+\cdots+\bar{1}}_{79})^{17} = \overline{79}$$

有 $79^{17} \equiv 79 \pmod{17}$，从而 $79^{17} \equiv 11 \pmod{17}$。

例 3.3 63^{11} 模 11 同余于多少？

解 11 是素数，于是域 $\mathbf{Z}_{11}$ 的特征为 11，从而在域 $\mathbf{Z}_{11}$ 中有

$$\overline{63^{11}} = \overline{63}^{11} = (\underbrace{\bar{1}+\bar{1}+\cdots+\bar{1}}_{63})^{11} = \overline{63}$$

有 $63^{11} \equiv 63 \pmod{11}$，从而 $63^{11} \equiv 8 \pmod{11}$。

从例 3.2 和例 3.3 受到启发，分析并且可以得到以下结论。

定理 3.1.2（费马小定理） 设 p 是素数，对于任一整数 a，都有

$$a^p \equiv a \pmod{p}$$

证明 根据素数的特性，对于任一整数 a，要么 $p \mid a$，要么 $(p,a)=1$。

若 $p \mid a$，则 $a \equiv 0 \pmod{p}$。同时，因为 $p \mid a$，则 $p \mid a^p$，且 $a^p \equiv 0 \pmod{p}$。根据模 p 同余等价关系的传递性 $\bar{a} \sim \bar{0}$，$\bar{0} \sim \bar{a}^p$，从而 $\bar{a} \sim \bar{a}^p$，即 $a^p \equiv a \pmod{p}$。

若$(p,a)=1$，即 $p\nmid a$，则 $a=qp+r$，$0<r<p$，在模 p 剩余类域 $\mathbf{Z}_p$ 中，有

$$\bar{a}=\overline{qp+r}=\bar{q}\,\bar{p}+\bar{r}=\bar{r}$$
$$=\underbrace{\bar{1}+\bar{1}+\cdots+\bar{1}}_{r}$$

根据域的性质 3.1.2 的推广$(a_1+a_2+\cdots+a_n)^p=a_1^p+a_2^p+\cdots+a_n^p$，$\forall a_i\in F$，有

$$\bar{a}^p=(\underbrace{\bar{1}+\bar{1}+\cdots+\bar{1}}_{r})^p=\bar{1}^p+\bar{1}^p+\cdots+\bar{1}^p=\bar{r}=\bar{a}$$

从而 $a^p\equiv a(\bmod p)$。

特别地，根据 2.4.1 节定理 2.4.1.1，在 $\mathbf{Z}_p$ 中，$(a,p)=1$，所以 $\bar{a}$ 是可逆元，在等式 $\bar{a}^p=\bar{a}$ 两边分别乘以 $\bar{a}$ 的逆元，左边为 $\bar{a}^p\,\bar{a}^{-1}=\bar{a}^{p-1}$，右边为 $\bar{a}\,\bar{a}^{-1}=\bar{1}$，两边相等，有 $\bar{a}^{p-1}=\bar{1}$，从而费马小定理变形为

$$a^{p-1}\equiv 1(\bmod p)$$

例 3.4 求 $2^{100}(\bmod 13)$。

解 $2^{100}(\bmod 13)\equiv 2^{12\times 8+4}\equiv(2^{12})^8 2^4\equiv(1)^8 2^4\equiv 3$

思考 1： 若 p 不是素数，$a^p\equiv a(\bmod p)$是否成立，请举例说明。

不成立，例如 $p=4$，则 $2^4\not\equiv 2(\bmod 4)$。

思考 2： 任一有限域 F 的元素个数 q 是多少？

定理 3.1.3* 任一有限域 F 的元素个数 q 一定是素数的指数幂，即 $q=p^n$，其中 p 为素数，n 为正整数。

证明* 设 F'是包含在 F 内的素域，因为有限域 F 的特征为 p，则 F'的特征也为 p。

设 F 作为 F'上的向量空间的维数为 n，取 F 在 F'上的一个基 $a_1,a_2,\cdots,a_n$，则 F 内每个元素 $\beta\in F$ 均可以唯一地表示成 $\beta=k_1a_1+k_2a_2+\cdots+k_na_n$，其中，$k_i\in F'$，$|F'|=p$，每个 k_i 均有 p 种取法，因此，全部系数组合共有 p^n 种取法。因为每种取法唯一的决定 F 内的元素，且不同取法得到的 F 内元素互不相同，所以 F 中元素的个数为 p^n 个。

3.2 环 $\mathbf{Z}_m$ 可逆元与欧拉函数

在 2.4.1 节，有如下结论：

定理 2.4.1.1 在模 m 剩余类环 $\mathbf{Z}_m$ 中，元素 $\bar{a}$ 是可逆元，当且仅当 a 与 m 互素，即 $(a,m)=1$。

若 $\mathbf{Z}_m$ 中，把所有可逆元组成的集合记作 $\mathbf{Z}_m^*$，那么集合 $\mathbf{Z}_m^*$ 中元素有多少个？

为回答上述问题，首先给出如下定义。

定义 3.2.1 模 m 剩余类环 $\mathbf{Z}_m$ 中，可逆元的个数记为 $\varphi(m)$，称 $\varphi(m)$为**欧拉函数**(Euler Function)。

根据定理 2.4.1.1，可以得到下面结论。

命题 3.2.1 $\varphi(m)$等于最小正完全剩余系$\{1,2,3,\cdots,m\}$中与 m 互素的整数的个数。

根据命题 3.2.1，很自然地会问欧拉函数 $\varphi(m)$的取值是多少？现从 m 为素数 p、素数幂 p^r 以及合数三个层面，进行探讨。

第一种情况，m 为素数 p。

观察下面三个例子，发现 $\varphi(3)=2$，$\varphi(5)=4$，$\varphi(7)=6$，可得如表 3-3 所示的结论。

表 3-3　m 为素数 p

m	最小正完全剩余系$\{1,2,3,\cdots,m\}$中与 m 互素的整数	欧拉函数 $\varphi(m)$
3	1,2	2
5	1,2,3,4	4
7	1,2,3,4,5,6	6

若 m 为素数 p，则 $\varphi(m)=p-1$。

证明　根据域的定义，若 p 是素数，则 $\mathbf{Z}_p$ 是一个域，从而 $\mathbf{Z}_p$ 中所有非零元都是可逆元，即

$$\mathbf{Z}_p^* = \{\bar{1},\bar{2},\cdots,\overline{p-1}\}$$

有 $\varphi(m)=p-1$。

第二种情况如表 3-4 所示，m 为素数幂 p^r。

表 3-4　m 为素数幂 p^r

m	最小正完全剩余系$\{1,2,3,\cdots,m\}$中与 m 互素的整数	欧拉函数 $\varphi(m)$
4	1,3	2
8	1,3,5,7	4
9	1,2,4,5,7,8	6

观察表 3-4 中的例子，分析后发现 $\varphi(4)=\varphi(2^2)=2^1\times(2-1)=2$，$\varphi(8)=\varphi(2^3)=2^2\times(2-1)=4$，$\varphi(9)=\varphi(3^2)=3^1\times(3-1)=6$，可得如下结论。

若 m 为素数幂 p^r，则 $\varphi(p^r)=p^{r-1}(p-1)$。

根据命题 3.2.1，$\varphi(p^r)$等于最小正完全剩余系$\{1,2,3,\cdots,p^r\}$中与 p^r 互素整数的个数，然而，哪些整数与 p^r 互素不好一一判断。这里可以通过逆向思维的方式，先计算$\{1,2,3,\cdots,p^r\}$中与 p^r 不互素整数的个数，最后，用总的个数减去不互素整数的个数，就是与 p^r 互素整数的个数。

在最小正完全剩余系$\{1,2,3,\cdots,p^r\}$中，任给 $a\in\{1,2,3,\cdots,p^r\}$，a 与 p^r 不互素，即 $(a,p^r)\neq 1$，为简化问题，可进一步把$(a,p^r)\neq 1$ 问题转换为$(a,p)\neq 1$。

若$(a,p)\neq 1$，根据素数的特性，有 $p\mid a$，等价于 $a=p,2p,3p,\cdots,p^{r-1}p$。从而$\{1,2,3,\cdots,p^r\}$中与 p^r 不互素整数的个数为 p^{r-1}个，于是

$$\varphi(p^r)=p^r-p^{r-1}=p^{r-1}(p-1)$$

现在问题的关键变成$(a,p^r)\neq 1\overset{?}{\Leftrightarrow}(a,p)\neq 1$。

证明　充分性$(a,p)\neq 1\Rightarrow(a,p^r)\neq 1$，因为$(a,p)\neq 1$，根据素数的特性，则有 $p\mid a$。又因为 $p\mid p^r$，表明 a 和 p^r 有公因数 p。根据互素的定义 2.3.3.1，知 a 和 p^r 不满足互素的条件 $c=\pm 1$，即 a 和 p^r 不互素$(a,p^r)\neq 1$，充分性满足。

必要性$(a,p^r)\neq 1\Rightarrow(a,p)\neq 1$，用逆否命题来证明。假设$(a,p)=1$，根据互素的性质 2.3.3.3，则有$(a,p^r)=1$，必要性满足。

第三种情况如表 3-5 所示，m 为合数。

表 3-5　m 为合数

m	最小正完全剩余系$\{1,2,3,\cdots,m\}$中与 m 互素的整数	欧拉函数 $\varphi(m)$
6	1,5	2
12	1,5,7,11	4
24	1,5,7,11,13,17,19,23	8

观察表 3-5 中的例子，发现 $\varphi(6)=\varphi(2\times3)=1\times2=2$，$\varphi(12)=\varphi(3\times4)=2\times2=4$，$\varphi(24)=\varphi(3\times8)=2\times4=8$，$\varphi(12)=\varphi(2\times6)=4\neq\varphi(2)\times\varphi(6)=1\times2$，$\varphi(24)=\varphi(4\times6)=8\neq\varphi(4)\times\varphi(6)=2\times2$，可得如下结论。

若 m 为合数，且 $m=pq$，$(p,q)=1$，则 $\varphi(m)=\varphi(p)\varphi(q)$。

最小正完全剩余系$\{1,2,3,\cdots,m\}$中，任给 $a\in\{1,2,3,\cdots,m\}$，哪些整数 a 和 m 互素不好一一判断，可以先判断$\{1,2,3,\cdots,m\}$中与 p 和 q 不互素的整数个数，最后，用总的个数减去不互素整数的个数，就是与 m 互素整数的个数。

证明　最小正完全剩余系$\{1,2,3,\cdots,pq\}$中，任给 $a\in\{1,2,3,\cdots,pq\}$，若$(a,p)\neq1$，根据素数的特性，有 $p\mid a$，等价于 $a=p,2p,3p,\cdots,qp$，从而$\{1,2,3,\cdots,pq\}$中与 p 不互素整数的个数为 q 个。类似地，$\{1,2,3,\cdots,pq\}$中与 q 不互素整数的个数为 p 个，其中，整数 pq 重复了一次，它既与 p 不互素，也与 q 不互素。因此，与 m 不互素整数的个数为 $p+q-1$ 个，可得与 m 互素整数的个数有 $m-(p+q-1)=pq-p-q+1=(p-1)(q-1)=\varphi(p)\varphi(q)$个，即 $\varphi(m)=\varphi(p)\varphi(q)$。

综上分析，可以得到如下结论。

定理 3.2.1　设 $m\in\mathbf{Z}^*$ 是一个大于 1 的整数，$\varphi(m)=|\mathbf{Z}_m^*|$。

(1) 若 m 为素数 p，则 $\varphi(p)=p-1$。

(2) 若 m 为素数幂 p^r，则 $\varphi(p^r)=p^{r-1}(p-1)$。

(3) 若 m 为合数，且 $m=pq$，$(p,q)=1$，则 $\varphi(m)=\varphi(p)\varphi(q)$。

结合算术基本定理，上述结论可以推广到任意大于 1 的整数 m。

推论 3.2.1　设 $m=p_1^{r_1}p_2^{r_2}\cdots p_n^{r_n}$，$p_1<p_2<\cdots<p_n$，其中，$p_1,p_2,\cdots,p_n$ 是两两不相等的素数，则

$$\varphi(m)=\varphi(p_1^{r_1})\varphi(p_2^{r_2})\cdots\varphi(p_n^{r_n})=\prod_{i=1}^{n}p_i^{r_i-1}(p_i-1)$$

例 3.5　求 $\varphi(77)$。

解　$\varphi(77)=\varphi(7)\varphi(11)=(7-1)\times(11-1)=6\times10=60$。

例 3.6　求 $\varphi(360)$。

解　$\varphi(360)=\varphi(2^3)\varphi(3^2)\varphi(5)=2^2\times(2-1)\times3\times(3-1)\times4=96$。

例 3.7　求 $\varphi(1800)$。

解　$\varphi(1800)=\varphi(2^3)\varphi(3^2)\varphi(5^2)=2^2\times(2-1)\times3\times(3-1)\times5^{2-1}\times(5-1)=480$。

例 3.8　求 $\varphi(49)$。

解　$\varphi(49)=\varphi(7^2)=7^{2-1}\times(7-1)=7\times6=42$。

3.3　$\mathbf{Z}_m^*$ 结构与群

当在模 m 剩余类 $\mathbf{Z}_m$ 中，定义了模 m 剩余类的加法以及乘法运算，模 m 剩余类组成的集合就是模 m 剩余类环，当 m 是素数 p 时，$\mathbf{Z}_p$ 是一个域。类似地，$\mathbf{Z}_m$ 中所有可逆元组成集合 $\mathbf{Z}_m^*$ 的结构是怎么样的，有没有加法和乘法运算？为回答这个问题，可以参考模 m 剩余类的加法以及乘法运算。

现从具体案例来探索上述问题。

在 $\mathbf{Z}_{12}^*=\{\bar{1},\bar{5},\bar{7},\overline{11}\}$ 中，有 $\bar{1}+\bar{5}=\bar{6}\notin\mathbf{Z}_{12}^*$，可以知模 12 剩余类的加法不是 $\mathbf{Z}_{12}^*$ 的运算。

模 12 剩余类的乘法是不是 $\mathbf{Z}_{12}^*$ 的运算呢？

$\bar{1}\ \bar{a}=\bar{a},\bar{a}\in\mathbf{Z}_{12}^*$。

$\bar{5}\ \bar{5}=\bar{1},\bar{5}\ \bar{7}=\overline{11},\bar{5}\ \overline{11}=\bar{7}$。

$\bar{7}\ \bar{7}=\bar{1},\bar{7}\ \overline{11}=\bar{5}$。

$\overline{11}\ \overline{11}=\bar{1}$。

根据上述运算，可知模 12 剩余类的乘法是 $\mathbf{Z}_{12}^*$ 的运算，且满足乘法结合律，有单位元 $\bar{1}$，每个元素都是可逆元，即每个元素有逆元。例如，$\bar{1}^{-1}=\bar{1},\bar{5}^{-1}=\bar{5},\bar{7}^{-1}=\bar{7},\overline{11}^{-1}=\overline{11}$，很自然地，可以提取出如下概念。

定义 3.3.1　设 G 是一个非空集合，如果 G 上定义了一种代数运算，通常称为乘法，并且满足以下 4 条运算法则：

(1) 封闭性，如果 $a,b\in G$，则 $ab\in G$。

(2) 乘法结合律，$(ab)c=a(bc),\forall a,b,c\in G$。

(3) 有单位元 e，G 中有一个元素 e，满足 $ea=ae=a,\forall a\in G$。

(4) G 中任一元素都是可逆元，即任给 $a\in G$，都有 $b\in G$，使得 $ab=ba=e$，此时 a 称为可逆元，b 是 a 的逆元，可记作 a^{-1}。

那么称 G 是一个**群**(Group)，该代数系统也可记作$(G,\cdot)$或者$<G,\cdot>$。

如果群 G 中，乘法运算还满足交换律，那么称 G 是一个**交换群**或者**阿贝尔群(Abel Group)**。

类似有限域的概念，如果群 G 中只含有限个元素，那么称 G 是**有限群**，并把有限群 G 所含元素的个数称为 G 的**阶**，可记作$|G|$，否则称 G 是**无限群**。

思考：$(G,\cdot)$关于乘法可构成乘法群，$(G,+)$关于加法可构成加法群吗？

在群 G 中，有乘法结合律，对于 $n\in\mathbf{N}^*$，有如下规定。

(1) $a^n:=\underbrace{aa\cdots a}_{n}$。

(2) $a^0:=e$。

(3) $a^{-n}:=(a^{-1})^n$。

根据上述规定，在群 G 中，逆元和幂运算 a^n 有如下性质。

(1) $(a^{-1})^{-1}=a$。

(2) 若 a 和 b 可逆，则 ab 可逆，且 ab 的逆元$(ab)^{-1}=b^{-1}a^{-1}$。

(3) $a^na^m=a^{n+m},n,m\in\mathbf{Z}$。

(4) $(a^n)^m=a^{nm}$，$n,m\in\mathbf{Z}$。

特别地，在交换群 G 中，有 $(ab)^n=a^nb^n$，$n\in\mathbf{Z}$，相反，若 G 不是交换群，$(ab)^n\neq a^nb^n$，$n\in\mathbf{Z}$。

到现在为止，从星期的案例，引出了环、域、群三种代数系统，为相关章节网络空间安全知识点提供了数学基础支撑。

有了上述定义，那么 $\mathbf{Z}_m^*$ 是一个交换群吗？可以从交换群的定义出发来分析。

(1) 封闭性，任取 $\bar{a},\bar{b}\in\mathbf{Z}_m^*$，因为 $\bar{a}$ 和 $\bar{b}$ 是可逆元，所以其逆元为 $\bar{a}^{-1}$ 和 $\bar{b}^{-1}$，找到一个元素 $(\bar{b}^{-1}\ \bar{a}^{-1})$，使得 $(\bar{a}\ \bar{b})(\bar{b}^{-1}\ \bar{a}^{-1})=\bar{1}$，因此 $\bar{a}$ 和 $\bar{b}$ 相乘的结果 $\bar{a}\ \bar{b}$ 还是可逆元，即 $\bar{a}\ \bar{b}\in\mathbf{Z}_m^*$。

(2) 模 m 剩余类 $\mathbf{Z}_m$ 中乘法满足结合律，所以 $\mathbf{Z}_m^*$ 的乘法满足结合律。

(3) 有单位元 $\bar{1}$，$\bar{1}\in\mathbf{Z}_m^*$。

(4) $\mathbf{Z}_m^*$ 中任一元素 $\bar{a}\in\mathbf{Z}_m^*$，有 $\bar{a}\ \bar{a}^{-1}=\bar{1}$，则 $\bar{a}^{-1}\in\mathbf{Z}_m^*$，满足 $\mathbf{Z}_m^*$ 中任一元素都是可逆元。

(5) 模 m 剩余类 $\mathbf{Z}_m$ 中乘法满足交换律，所以 $\mathbf{Z}_m^*$ 的乘法满足交换律。

综上分析，$\mathbf{Z}_m^*$ 的结构就比较清楚了，$\mathbf{Z}_m^*$ 是一个交换群，且阶为欧拉函数 $\varphi(m)$，该结论可以总结如下。

命题 3.3.1 $\mathbf{Z}_m^*$ 是一个交换群，其阶为欧拉函数 $\varphi(m)$。

例 3.9 求 $\mathbf{Z}_9^*$ 的阶。

解 $\mathbf{Z}_9^*$ 的阶为 $\varphi(9)=\varphi(3^2)=3^{2-1}\times(3-1)=6$。

例 3.10 求 $\mathbf{Z}_{35}^*$ 的阶。

解 $\mathbf{Z}_{35}^*$ 的阶为 $\varphi(35)=\varphi(5)\varphi(7)=(5-1)\times(7-1)=24$。

3.4 欧拉定理与元素的阶

在例 3.9 中，知道 $\mathbf{Z}_9^*$ 的阶为 6，那么 $\mathbf{Z}_9^*$ 元素的 r 次幂分别是多少呢？因为 $\mathbf{Z}_9^*$ 的阶为 6，r 次幂取值从 1 到 6，详情如表 3-6 所示。

表 3-6 $\mathbf{Z}_9^*$ 元素 $\bar{a}$ 的 r 次幂

$\bar{a}$	$\bar{a}^2$	$\bar{a}^3$	$\bar{a}^4$	$\bar{a}^5$	$\bar{a}^6$	$\varphi(m)$	元素的阶
$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	$\bar{1}$	6	1
$\bar{2}$	$\bar{4}$	$\bar{8}$	$\bar{7}$	$\bar{5}$	$\bar{1}$	6	6
$\bar{4}$	$\bar{7}$	$\bar{1}$	$\bar{4}$	$\bar{7}$	$\bar{1}$	6	3
$\bar{5}$	$\bar{7}$	$\bar{8}$	$\bar{4}$	$\bar{2}$	$\bar{1}$	6	6
$\bar{7}$	$\bar{4}$	$\bar{1}$	$\bar{7}$	$\bar{4}$	$\bar{1}$	6	3
$\bar{8}$	$\bar{1}$	$\bar{8}$	$\bar{1}$	$\bar{8}$	$\bar{1}$	6	2

观察表 3-6 中具体的值，探讨里面蕴含的规律或者结论。

1. 欧拉定理

观察和分析发现，在表 3-6 中，群 $\mathbf{Z}_9^*$ 的阶为 6，所有元素到 $\varphi(m)=6$ 次方，都等于单位元 $\bar{1}$，很自然地推测有如下结论。

命题 3.4.1　在 n 阶群 G 中，对于任意 $a\in G$，有

$$a^n=e$$

其中，e 是群 G 的单位元。

根据命题 3.4.1 结论 $a^{|G|}=e$，其中 $n=|G|$。在群 $\mathbf{Z}_m^*$ 中，任取 $\bar{a}\in\mathbf{Z}_m^*$，有 $\bar{a}^{\varphi(m)}=\bar{1}$，其中，$n=|G|=\varphi(m)$，可以立即得到欧拉定理。

定理 3.4.1（欧拉定理）　设 m 是大于 1 的正整数，如果整数 a 与 m 互素，则

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

证明　由于 $(a,m)=1$，根据可逆元的判定，在 $\mathbf{Z}_m^*$ 中，$\bar{a}$ 是可逆元，即 $\bar{a}\in\mathbf{Z}_m^*$。又有 $\mathbf{Z}_m^*$ 的阶 $|\mathbf{Z}_m^*|=\varphi(m)$，根据命题 3.4.1，则 $\bar{a}^{\varphi(m)}=e=\bar{1}$，从而 $\overline{a^{\varphi(m)}}=\bar{1}$，于是有

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

该证明利用了有限群结构的相关知识，较简便地给出了欧拉定理的一种证明。

例 3.11　设 $m=9,a=2$，根据欧拉定理，给出模 m 下关于 a 的同余式。

解　$m=9,a=2$，有 $(m,a)=1,\varphi(m)=\varphi(8)=\varphi(3^2)=8$，则 $a^{\varphi(m)}\equiv 2^8\equiv 1(\bmod 9)$。

例 3.12　设 $m=11,a=2$，根据欧拉定理，给出模 m 下关于 a 的同余式。

解　$m=11,a=2$，有 $(m,a)=1,\varphi(m)=\varphi(11)=10$，则 $a^{\varphi(m)}\equiv 2^{10}\equiv 1(\bmod 11)$。

2. 元素的阶

在 $\mathbf{Z}_9^*$ 中，$\bar{1}^1=\bar{1},\bar{2}^6=\bar{1},\bar{4}^3=\bar{1},\bar{5}^6=\bar{1},\bar{7}^3=\bar{1},\bar{8}^2=\bar{1}$，分析发现，每个元素在有限次方之后都等于单位元。

根据上述分析，可以提取出如下概念。

定义 3.4.1　设 G 是一个群，对于 $a\in G$，如果存在正整数 n，使得 $a^n=e$，则称 a 是**有限阶元素**(Element of Finite Order)，使 $a^n=e$ 成立的最小正整数 n 称为 a 的**阶**(Order)，可记作 $|a|$，或者 ord(a)，如果不存在这样的 n，则称 a 是**无限阶元素**(Element of Infinite Order)。

观察表 3-6，可以很容易判断出 $|\bar{1}|=1,|\bar{2}|=6,|\bar{4}|=3,|\bar{5}|=6,|\bar{7}|=3,|\bar{8}|=2$，若元素 a 的阶为 n，有 $a^n=e$，并进一步观察到，如果 $n|m$，则 $a^m=e$，例如，$\bar{4}^3=\bar{1}$，且 $3|6$，则 $\bar{4}^6=\bar{1};\bar{8}^2=\bar{1}$，且 $2|4,2|6$，则 $\bar{8}^4=\bar{1},\bar{8}^6=\bar{1}$。由此，可以得到下面结论。

定理 3.4.2　设 G 是一个群，$a\in G$，若 a 的阶为 n，则 $a^m=e$ 当且仅当 $n|m$，其中，e 是 G 的单位元。

证明　充分性，由于 $n|m$，因此存在整数 $q\in\mathbf{Z}$，使得 $m=qn$，于是有

$$a^m=a^{qn}=(a^n)^q=e^q=e$$

必要性，如果 $a^m=e$，根据带余除法，令 $m=qn+r,0\leqslant r<n$，由于

$$e=a^m=a^{qn+r}=(a^n)^q a^r=ea^r=a^r$$

因为 $e=a^r$，根据群的规定 $a^0=e$，则 $r=0$，从而 $m=qn+0=qn$，即 $n|m$。

特别地，有限群 G 每个元素的阶 n 是群 G 的阶 $|G|$ 的因子，即 $n||G|$，则对于任意 $a\in G$，有 $a^{|G|}=e$，即命题 3.4.1 的结论。

当 G 是交换群或阿贝尔群时，常把群 G 的运算记成加法，并且满足以下 4 条运算法则：

(1) 封闭性，如果 $a,b\in G$，则 $a+b\in G$。

(2) 加法结合律，$(a+b)+c=a+(b+c),\forall a,b,c\in G$。

(3) 有零元，可记作 0，满足 $0+a=a+0=a$，$\forall a\in G$。

(4) G 中任一元素都有负元，即任意 $a\in G$，都有 $b\in G$，使得 $a+b=b+a=0$，此时，把 b 称为 a 的负元，可记作 $-a$。

那么称 G 是一个群，该代数系统也可记作$(G,+)$或者$<G,+>$。

在群 G 中，若把群 G 的运算记成加法，对于 $n\in\mathbf{N}^*$，有如下规定。

(1) $na:=\underbrace{a+a+\cdots+a}_{n}$。

(2) $0a:=0$。

(3) $(-n)a:=n(-a)$。

为什么把群 G 上的运算定义为加法？因为运算对象有时自身满足加法运算。

例 3.13 非 0 实数集 $\mathbf{R}^*$ 是否形成群？

解 $\mathbf{R}^*$ 对乘法运算满足封闭性和结合律，单位元为 1，任意 $a\in\mathbf{R}^*$ 的逆元 $a^{-1}=1/a$，因此$<\mathbf{R}^*,\cdot>$形成群，且是交换群。

类似地，非 0 有理数集 $\mathbf{Q}^*$、非 0 复数集 $\mathbf{C}^*$ 对乘法也构成交换群。

例 3.14 整数集 $\mathbf{Z}$ 是否形成群？

解 $\mathbf{Z}$ 对加法运算满足封闭性和结合律，零元为 0，$a\in\mathbf{Z}$ 的负元是 $-a$，因此$<\mathbf{Z},+>$形成群，且是无限交换群。

注意，$\mathbf{Z}$ 对乘法运算不能构成群，因为除 ±1 外，其他元素均没有逆元。

类似地，有理数集 $\mathbf{Q}$、实数集 $\mathbf{R}$ 和复数集 $\mathbf{C}$ 对通常意义下的加法也构成交换群，零元为 0，a 的负元为 $-a$。

例 3.15 模 m 剩余类环 $\mathbf{Z}_m$ 是否形成加法群？

解 模 m 剩余类的加法成为一个群，且是交换群，因为模 m 剩余类的加法运算满足封闭性和结合律，零元为 0，$\bar{a}\in\mathbf{Z}_m$ 的负元是 $-\bar{a}$。

模 m 剩余类的乘法不成为一个群，因为零元 0 没有逆元。

根据例 3.15，可以得到如下结论。

任给一个环 R，R 对于加法成为一个群，可记作$<R,+>$。

到此为止，已介绍环、域和群 3 种基本代数结构，各种代数结构的关系如图 3-1 所示。

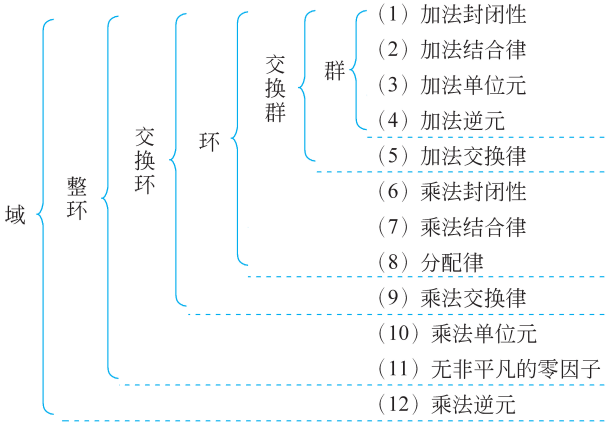

图 3-1 群、环、域的关系

3.5　原根与阶

由欧拉定理可知，若整数 a 与 m 互素，则 $a^{\varphi(m)} \equiv 1 \pmod{m}$，那么思考如下问题：在模运算中，$\varphi(m)$ 是否是使得 $a^? \equiv 1 \pmod{m}$ 成立的最小正整数？通过例子 $2^3 \equiv 1 \pmod{7}$，$\varphi(7)=6$，知 $\varphi(m)$ 不是使得 $a^? \equiv 1 \pmod{m}$ 成立的最小正整数。那么在模运算中，这个最小正整数有什么性质？如何求这个最小的正整数呢？

定义 3.5.1　设 $a, m \in \mathbf{Z}, m>1, (a,m)=1$，则使得

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

成立的最小正整数 n 称为 a 对模 m 的**阶**，记作 $\mathrm{ord}_m(a)$，或者 $\delta_m(a)$。

阶翻译自英文单词 order，该术语来自抽象代数(Abstract Algebra)的群论，抽象代数又称近世代数，元素的阶详情见 3.4 节定义 3.4.1。

定义 3.5.2　若 a 对模 m 的阶 $n=\mathrm{ord}_m(a)=\varphi(m)$，则 a 称为模 m 的**原根**(Primitive Root)。

根据上述两个定义，在模运算中，阶指的是 $a^n \equiv 1 \pmod{m}$ 同余式中满足条件的“n”，而原根指的是 $a^n \equiv 1 \pmod{m}$ 同余式中满足条件的“a”，也就是底数。

下面根据定义求模运算中的阶和原根。

根据定义求 a 对模 m 的阶，已知 $a, m \in \mathbf{Z}, m>1, (a,m)=1$，先计算 $a \pmod{m}$，$a^2 \pmod{m}, \cdots, a^{\varphi(m)} \pmod{m}$ 的值，然后，判断使 $a^n \equiv 1 \pmod{m}$ 成立的最小正整数 n，即为 a 对模 m 的阶。

根据欧拉定理知，$(a,m)=1, a^{\varphi(m)} \equiv 1 \pmod{m}$，故 a 对模 m 的阶一定存在，但是对于求模 m 的原根，可通过计算模 m 的最小正简化剩余系中的所有整数 a 对模 m 的阶 n，来判断 a 是否为模 m 的原根。

例 3.16　若整数 $m=7$，求 a 对模 m 的阶和模 7 的原根。

解　若整数 $m=7$，则 $\varphi(7)=6$。

计算模 m 最小正简化剩余系中的所有整数 a，即 $1,2,\cdots,m$ 中与 m 互素的所有整数组成的集合 $\{1,2,3,4,5,6\}$。

计算 a 对模 m 的阶 n：

$1^1 \equiv 1 \pmod{7}$

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

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

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

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

$6^1 \equiv 6 \pmod{7}, 6^2 \equiv 1 \pmod{7}$

则 1、2、3、4、5、6 对模 7 的阶分别为 1、3、6、3、6、2。

根据原根的定义可知，3 和 5 是模 7 的原根。

例 3.17　若整数 $m=14$，求 a 对模 m 的阶和模 14 的原根。

解 若整数 $m=14$，则 $\varphi(14)=6$。

计算模 m 最小正简化剩余系中的所有整数 a，即 $1,2,\cdots,m$ 中与 m 互素的所有整数组成的集合$\{1,3,5,9,11,13\}$。

计算 a 对模 m 的阶 n：

$$1^1 \equiv 1(\bmod 14)$$
$$3^3 \equiv -1(\bmod 14), 3^6 \equiv 1(\bmod 14)$$
$$5^3 \equiv -1(\bmod 14), 5^6 \equiv 1(\bmod 14)$$
$$9^3 \equiv 1(\bmod 14),$$
$$11^3 \equiv 1(\bmod 14)$$
$$13^2 \equiv 1(\bmod 14)$$

则 1、3、5、9、11、13 对模 14 的阶分别为 1、6、6、3、3、2。

根据原根的定义可知，3 和 5 是模 14 的原根。

例 3.18 若整数 $m=15$，求 a 对模 m 的阶和模 15 的原根。

解 若整数 $m=15$，则 $\varphi(15)=8$。

计算模 m 最小正简化剩余系中的所有整数 a，即 $1,2,\cdots,m$ 中与 m 互素的所有整数组成的集合$\{1,2,4,7,8,11,13,14\}$。

计算 a 对模 m 的阶 n：

$$1^1 \equiv 1(\bmod 15)$$
$$2^4 \equiv 1(\bmod 15)$$
$$4^2 \equiv 1(\bmod 15)$$
$$7^4 \equiv 1(\bmod 15)$$
$$8^4 \equiv 1(\bmod 15)$$
$$11^2 \equiv 1(\bmod 15)$$
$$13^4 \equiv 1(\bmod 15)$$
$$14^2 \equiv 1(\bmod 15)$$

则 1、2、4、7、8、11、13、14 对模 15 的阶分别为 1、4、2、4、4、2、4、2。

根据原根的定义可知，模 15 没有原根。

下面介绍阶和原根的一些性质，根据 3.4 节定理 3.4.2，易得如下两个结论。

定理 3.5.1 设 $a,m\in\mathbf{Z},m>1,(a,m)=1,n$ 为正整数，则 $a^n\equiv 1(\bmod m)$的充分必要条件是$\mathrm{ord}_m(a)\mid n$。

推论 3.5.1 设 $a,m\in\mathbf{Z},m>1,(a,m)=1$，则 $\mathrm{ord}_m(a)\mid\varphi(m)$。

例 3.19 求整数 5 对模 17 的阶 $\mathrm{ord}_{17}(5)$。

解 根据题目条件，由 $m=17,a=5,(5,17)=1$，则欧拉函数 $\varphi(m)=16$。由推论 3.5.1 可知，$\mathrm{ord}_m(a)\mid\varphi(m)$，即 $\mathrm{ord}_{17}(5)\mid 16$，则 $\mathrm{ord}_{17}(5)$可能等于 1、2、4、8 或 16。把 $\mathrm{ord}_{17}(5)$所有可能的值代入 $5^n(\bmod 17)$计算，其中 $n=\mathrm{ord}_{17}(5)=1,2,4,8,16$。

$$5^1=5(\bmod 17),\quad 5^2=8(\bmod 17),\quad 5^4=-4(\bmod 17),$$
$$5^8=-1(\bmod 17),\quad 5^{16}=1(\bmod 17)$$

根据阶的定义 3.5.1，知 $\mathrm{ord}_{17}(5)=16$。

另外，根据原根的定义，知 5 是模 17 的原根。

注意，原根又称为本原元或者生成元(Generator)，原根的英文可能觉得不好理解，如果称为生成元，可能更容易理解这个“本原”的含义，即可以生成群中其他所有元素的“本原元”，详情见 3.6 节生成元内容。

3.6　循环群与生成元

观察表 3-6，可以看到有两个特殊的元素 $\overline{2}$ 和 $\overline{5}$，$\overline{2}^1=\overline{2}$，$\overline{2}^2=\overline{4}$，$\overline{2}^3=\overline{8}$，$\overline{2}^4=\overline{7}$，$\overline{2}^5=\overline{5}$，$\overline{2}^6=\overline{1}$，分析发现，$\mathbf{Z}_9^*$ 中的元素都可以用 $\overline{2}$ 的方幂来表示，即 $\mathbf{Z}_9^*=\{\overline{2}^1,\overline{2}^2,\overline{2}^3,\overline{2}^4,\overline{2}^5,\overline{2}^6\}$。

根据上述分析，可以提取出如下概念。

定义 3.6.1　设 G 是一个群，$a\in G$，若 G 中每个元素都能写成 a 的方幂的形式，则称 G 是**循环群**(Cyclic Group)，称 a 为 G 的一个**生成元**，此时，可以把 G 记作$<a>$。

例如，在循环群 $\mathbf{Z}_9^*$ 中，元素 $\overline{2}$ 和 $\overline{5}$ 都是生成元，可以把循环群 $\mathbf{Z}_9^*$ 记作$<\overline{2}>$或者$<\overline{5}>$。

根据定义 3.6.1，可以得到下述结论。

(1) 设 G 是一个有限群，$a\in G$，若元素 a 的阶 $|a|$ 等于群 G 的阶 $|G|$，则 G 是循环群，a 是群 G 的一个生成元。

(2) 设 G 是一个有限循环群，则 a 是群 G 的生成元当且仅当元素 a 的阶等于 $|G|$。

(3) 循环群一定是交换群，交换群不一定是循环群。

例如，交换群 $\mathbf{Z}_8^*=\{\overline{1},\overline{3},\overline{5},\overline{7}\}$不是循环群，因为 $\mathbf{Z}_8^*$ 中元素的阶，$\overline{1}^1=\overline{1}$，$\overline{3}^2=\overline{1}$，$\overline{5}^2=\overline{1}$，$\overline{7}^2=\overline{1}$，没有一个等于群 $\mathbf{Z}_8^*$ 的阶 4。

注意，当交换群 G 的运算记为加法时，若有一个元素 $a\in G$，使得 G 中每个元素 b 都能写成 a 的整数倍的形式，即 $b=ka$，那么 G 是循环群，称 a 为 G 的一个生成元。

从上面的例子，知道 $\mathbf{Z}_8^*$ 不是循环群，$\mathbf{Z}_9^*$ 是循环群。

思考：$\mathbf{Z}_m^*$ 中 m 取值多少时，$\mathbf{Z}_m^*$ 是循环群？

观察表 3-7，当 $m=2$ 和 $m=4$ 时，$\mathbf{Z}_m^*$ 是循环群，当 $m=8=2^3$ 时，$\mathbf{Z}_8^*$ 不是循环群，表明 2 的方幂只有为 1 次方和 2 次方时，即 $m=2^1$ 和 $m=2^2$ 时，$\mathbf{Z}_m^*$ 是循环群。

表 3-7　$\mathbf{Z}_m^*$ 循环群判定

$\mathbf{Z}_m^*$	$\mathbf{Z}_m^*$ 中元素	$<a>$	是否为循环群
$\mathbf{Z}_2^*$	$\{\overline{1}\}$	$\{\overline{1}^1\}$	是
$\mathbf{Z}_3^*$	$\{\overline{1},\overline{2}\}$	$\{\overline{2}^2,\overline{2}^1\}$	是
$\mathbf{Z}_4^*$	$\{\overline{1},\overline{3}\}$	$\{\overline{3}^2,\overline{3}^1\}$	是
$\mathbf{Z}_5^*$	$\{\overline{1},\overline{2},\overline{3},\overline{4}\}$	$\{\overline{2}^4,\overline{2}^1,\overline{2}^3,\overline{2}^2\}$	是
$\mathbf{Z}_6^*$	$\{\overline{1},\overline{5}\}$	$\{\overline{5}^2,\overline{5}^1\}$	是
$\mathbf{Z}_7^*$	$\{\overline{1},\overline{2},\overline{3},\overline{4},\overline{5},\overline{6}\}$	$\{\overline{3}^6,\overline{3}^2,\overline{3}^1,\overline{3}^4,\overline{3}^5,\overline{3}^3\}$	是
$\mathbf{Z}_8^*$	$\{\overline{1},\overline{3},\overline{5},\overline{7}\}$	$\overline{1}^1=\overline{1},\overline{3}^2=\overline{1},\overline{5}^2=\overline{1},\overline{7}^2=\overline{1}$	否
$\mathbf{Z}_9^*$	$\{\overline{1},\overline{2},\overline{4},\overline{5},\overline{7},\overline{8}\}$	$\{\overline{2}^6,\overline{2}^1,\overline{2}^2,\overline{2}^5,\overline{2}^4,\overline{2}^3\}$	是
$\mathbf{Z}_{12}^*$	$\{\overline{1},\overline{5},\overline{7},\overline{11}\}$	$\overline{1}^1=\overline{1},\overline{5}^2=\overline{1},\overline{7}^2=\overline{1},\overline{11}^2=\overline{1}$	否
$\mathbf{Z}_{18}^*$	$\{\overline{1},\overline{5},\overline{7},\overline{11},\overline{13},\overline{17}\}$	$\{\overline{5}^6,\overline{5}^1,\overline{5}^2,\overline{5}^5,\overline{5}^4,\overline{5}^3\}$	是

当 m 为奇素数 p 时，例如，$p=5$ 和 $p=7$，$\mathbf{Z}_m^*$ 是循环群。当 $p=9=3^3$，即 $m=p^r$ 时，$\mathbf{Z}_m^*$ 也是循环群。

当 m 为 $2p^r$ 时，例如，$m=6=2\times3^1$，$m=18=2\times3^2$，$\mathbf{Z}_m^*$ 也是循环群。

根据上述分析，可以得到如下结论。

定理 3.6.1 $\mathbf{Z}_m^*$ 是循环群当且仅当 m 为下列情形之一：$m=2$，$m=4$，$m=p^r$，$m=2p^r$，其中，$m>1$，p 是奇素数，$r\in\mathbf{N}^*$。

例 3.20 加法群 $\mathbf{Z}_m$ 是否为循环群？

解 根据例 3.15，模 m 剩余类环 $\mathbf{Z}_m$ 对于加法成为一个交换群，又由于 $\bar{b}=\underbrace{\bar{1}+\bar{1}+\cdots+\bar{1}}_{k}=k\bar{1}$，$1\leqslant k\leqslant m$，因此加法群 $\mathbf{Z}_m$ 是循环群，$\bar{1}$ 为 $\mathbf{Z}_m$ 的一个生成元。

类似地，根据例 3.14，$\mathbf{Z}$ 对加法形成群，又由于 $b=k1$，$\forall k\in\mathbf{Z}$，因此加法群 $<\mathbf{Z},+>$ 也是循环群，1 为 $\mathbf{Z}$ 的一个生成元。

例 3.21 求循环群 $\mathbf{Z}_5^*$ 的一个生成元。

解 根据表 3-7，知道 $\bar{2}^2=\bar{4}$，$\bar{2}^3=\bar{3}$，$\bar{2}^4=\bar{1}$，有 $|\bar{2}|=4=\varphi(5)=|\mathbf{Z}_5^*|$，得到 $\bar{2}$ 是 $\mathbf{Z}_5^*$ 的一个生成元。

注意，$\bar{3}$ 也是 $\mathbf{Z}_5^*$ 的一个生成元。

例 3.22 求循环群 $\mathbf{Z}_{17}^*$ 的一个生成元。

解 根据例 3.19，知 $\bar{5}$ 是 $\mathbf{Z}_{17}^*$ 的一个生成元。

注意，该群的生成元总共有 $\varphi(|\mathbf{Z}_{17}^*|)=\varphi(16)=\varphi(2^4)=2^{4-1}\times(2-1)=8$ 个。

定理 3.6.2* 设 $G=<a>$ 是循环群。

(1) 若 $G=<a>$ 是无限循环群，则 G 只有两个生成元，即 a 和 a^{-1}。

(2) 若 $G=<a>$ 是 n 阶循环群，即 $G=\{e,a^1,a^2,\cdots,a^{n-1}\}$，则 a^k 是群 G 的生成元当且仅当 k 与 n 互素 $(k,n)=1$，其中，$k\in\{1,2,3,\cdots,n-1\}$。

易知，n 阶循环群生成元的个数为 $\varphi(n)$。

例 3.23 $<\mathbf{Z},+>$ 是否为交换群和无限循环群？若是，指出其单位元、逆元和生成元。

解 $<\mathbf{Z},+>$ 是交换群，单位元是 0，a 的加法逆元是 $-a$，也是无限循环群，生成元是 1 和 -1，两者互为逆元。

3.7 代数系统在网络空间安全中的应用

前面已经学习了环、域和群三种代数系统，这三种代数系统为网络空间安全提供了重要的密码学数学基础，例如，模 n 剩余类环 $\mathbf{Z}_n$ 上的 RSA 公钥密码体制，有限域上的 ElGamal 公钥密码体制等。

3.7.1 RSA 公钥密码体制

1977 年，RSA 公钥密码体制由 MIT 的 Ronald L. Rivest、Adi Shamir 和 Leonard

Adleman 在 MIT 的技术报告中提出，正式发表于 1978 年的 *Communication of ACM*[①]，是第一个也是当今应用最广泛的公钥密码体制之一，既可用于加密，也可用于数字签名。

RSA 算法利用了单向陷门函数(One-Way Trapdoor Function)的原理，该函数包含两个明显特征：一是单向性，二是存在陷门。

单向性，也称不可逆性，即对于一个函数 $y=f(x)$，若已知 x 要计算出 y 非常容易，但是已知 y 要计算出 $x=f^{-1}(y)$则很困难。

陷门，也称为后门。对于单向函数，若存在一个 z，假设知道 z，则可容易地计算出 $x=f^{-1}(y)$，假设不知道 z，则无法计算出 $x=f^{-1}(y)$，因此称函数 $y=f(x)$为单向陷门函数，其中，z 称为陷门。

RSA 算法安全性依赖大整数因子分解难题，其原理如图 3-2 所示。已知两个大素数 p 和 q，计算 $n=p\times q$ 是容易的，但是，已知一个大整数，如长度为 1024 位的整数，采用蛮力分解出 p 和 q 两个因子是困难的，当前暂还没有快速有效的大整数因子分解方法。

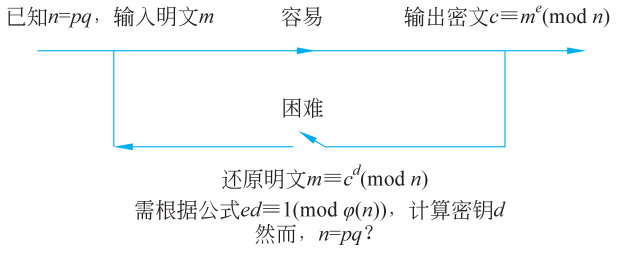

图 3-2　RSA 算法原理示意图

RSA 算法过程如图 3-3 所示。假设用户 A 要和 B 通信，B 拥有一对密钥(e,d)，其中，e 为公钥，d 为私钥，A 要传输的明文数据为 $\bar{m}$，$\bar{m}\in\mathbf{Z}_n$。首先，A 用 B 的公钥 e 对 $\bar{m}$ 加密之后得到密文 c，注意，在模 m 剩余类环中，有加法和乘法两种运算，这里选择乘法运算，若选择加法运算，知道 n 和公钥 e 之后，可以很容易求出私钥 d，不安全。然后，A 把密文 c 发送给 B。B 收到密文 c 之后，希望能够用私钥 d 解密密文 c，还原出明文 $\bar{m}$。

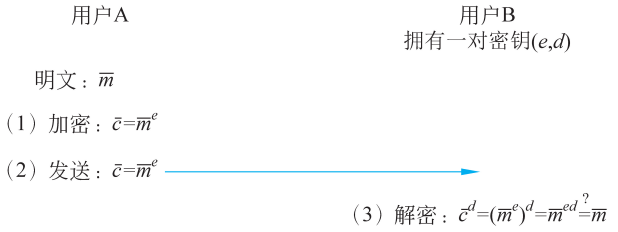

图 3-3　RSA 算法过程示意图

从图 3-3 中可以知道，现在问题的关键是：考虑公钥 e 和私钥 d 满足什么条件时，明文 $\bar{m}$ 加密并解密之后，成功还原出明文，即

$$\bar{m}^{ed}=\bar{m} \tag{1}$$

下面分两种情况来讨论，情形一：$\bar{m}$ 为可逆元；另一种情形：$\bar{m}$ 不是可逆元。

---

① R. L. Rivest, A. Shamir, and L. Adleman. 1978. A method for obtaining digital signatures and public-key cryptosystems. Commun. ACM 21,2 (Feb. 1978),120-126. https://doi.org/10.1145/359340.359342.

情形一： $\bar{m}$ 为可逆元，即 $\bar{m}\in\mathbf{Z}_n^*$，$(m,n)=1$。

根据命题 3.4.1，在交换群 $\mathbf{Z}_n^*$ 中，有 $\bar{m}^{\varphi(n)}=\bar{1}$，则 $\bar{m}^{k\varphi(n)}=\bar{1}^k=\bar{1}$，$k\in\mathbf{Z}$。在该式左右两边同乘 $\bar{m}$，则有

$$\bar{m}^{k\varphi(n)}\bar{m}=\bar{m}\Leftrightarrow\bar{m}^{k\varphi(n)+1}=\bar{m} \tag{2}$$

对比式(1)和式(2)，若要使得式(1)成立，只需令 $k\varphi(n)+1=ed$，$k\in\mathbf{Z}$，即 $ed\equiv1(\bmod\varphi(n))$，则 $\bar{m}^{k\varphi(n)+1}=\bar{m}^{ed}=\bar{m}$。

注意，在条件 $k\varphi(n)+1=ed$，$k\in\mathbf{Z}$ 中，由于 $de-k\varphi(n)=1$，从而 $(e,\varphi(n))=1$，蕴含着公钥 e 和 $\varphi(n)$ 互素的条件。

综上分析，对情形一，若 $ed\equiv1(\bmod\varphi(n))$，则 $\bar{m}^{ed}=\bar{m}$。

情形二： $\bar{m}$ 不是可逆元，即 $\bar{m}\notin\mathbf{Z}_n^*$。

$\bar{m}\notin\mathbf{Z}_n^*$，即 $(m,n)\neq1$，由于 $n=pq$，(m,n) 的公因数一定整除 n，即 $(m,n)\mid n$，则 m 和 n 的公因数要么为 p，要么为 q。

注意，如果 m 和 n 的公因数为 p 和 q，则 m 是 p 的倍数，也是 q 的倍数，从而是 pq 的倍数，与 $m<n=pq$ 矛盾。类似地，如果 m 和 n 的公因数为 n，也与 $m<n$ 矛盾，一个大的数 n，不可能整除一个小的数 m。

若 $(m,n)=p$，有 $p\mid m$，且 $q\nmid m$。根据素数的特性，即定理 2.3.3.2，有 $(m,q)=1$。根据命题 3.4.1，在交换群 $\mathbf{Z}_q^*$ 中，有 $\bar{m}^{\varphi(q)}=\bar{1}$，则 $\bar{m}^{k\varphi(q)}=\bar{1}^k=\bar{1}$，$[\bar{m}^{k\varphi(q)}]^{\varphi(p)}=\bar{1}$，$\bar{m}^{k\varphi(n)}=\bar{1}$，即

$$m^{k\varphi(n)}\equiv1(\bmod q),\quad k\in\mathbf{Z} \tag{3}$$

所以，存在一个整数 r，使得 $m^{k\varphi(n)}=1+rq$，两边同时乘以 m，令 $m=jp$，$j\in\mathbf{Z}$，得

$$m^{k\varphi(n)+1}=m+rqm=m+rqjp=m+rjn \tag{4}$$

式(4)中，rj 为整数，上式可写成 $m^{k\varphi(n)+1}\equiv m(\bmod n)$。

当 $ed=k\varphi(n)+1$ 时，则 $m^{ed}\equiv m(\bmod n)$，即 $\bar{m}^{ed}=\bar{m}$，得证。

若 $(m,n)=q$，证明类似。

综上分析，当 $ed\equiv1(\bmod\varphi(n))$ 时，无论 $\bar{m}$ 是否为可逆元，RSA 算法都能对输入明文 $\bar{m}$ 正确地进行加解密。

1. RSA 算法详情

RSA 算法主要包括密钥生成、加密和解密三个关键步骤，各个步骤的详情如下。

1) 密钥生成

① 选取两个大素数 p 和 q，如长度都接近 512 位。

② 计算乘积 $n=pq$，$\varphi(n)=(p-1)(q-1)$，其中，欧拉函数 $\varphi(n)$ 为 $\mathbf{Z}_n$ 中可逆元的个数。

③ 随机选择一个整数 e，$1<e<\varphi(n)$，要求 e 与 $\varphi(n)$ 互素，即 $(e,\varphi(n))=1$。

④ 根据扩展欧几里得算法计算私钥 d，以满足 $ed\equiv1(\bmod\varphi(n))$。

⑤ 公钥为 e 和 n，对外发布，私钥为 d，保留。同时，素数 p 和 q 不能泄露。

2) 加密

明文可以先转换为二进制比特串，根据分组长度 $l=length(m_i)\leqslant\log_2^n$，再转换为十进制分组，以确保每个分组对应的十进制数小于 n。然后，对每个明文分组 m_i 做加密运算。

例如，若明文为“OK”，根据 ASCII 编码，先转换为二进制比特串“0100111101001011”，如果 $n=256$，可以取 $l=8$，再转换为十进制分组“79”和“75”，确保每个分组的值小于 256，

然后，分别对每个十进制分组加密。

加密过程如下。

① 获得公钥(e,n)。

② 把输入明文 m 分为 t 组，$m=m_1m_2\cdots m_i\cdots m_t$，每组长度 $l=length(m_i)\leqslant\log_2^n$。

③ 对每个明文分组加密，$c_i\equiv m_i^e(\bmod n)$，得到输出密文 $c=c_1c_2\cdots c_i\cdots c_t$。

其中，m 是输入明文，c 是输出密文。

3）解密

① 输入为密文分组 $c=c_1c_2\cdots c_i\cdots c_t$。

② 对每个密文分组进行解密，$m_i\equiv c_i^d(\bmod n)$，解密还原得到明文 $m=m_1m_2\cdots m_i\cdots m_t$。

RSA 算法伪代码描述如下。

RSA Algorithm

输入：明文 m，素数 p 和 q。

输出：加密解密后，输出明文 m。

(1) 计算欧拉函数 $\varphi(n)$，$\varphi(n)=(p-1)(q-1)$

(2) 随机选择公钥 e，$e\leftarrow(e,\varphi(n))=1$

(3) 计算私钥 d，$d\leftarrow ed\equiv 1(\bmod \varphi(n))$

(4) 加密明文，得到密文 c，$c\leftarrow m^e(\bmod n)$

(5) 解密 c，得到明文 m，$m\leftarrow m\equiv c^d(\bmod n)$

例 3.24　取两个素数 $p=7$，$q=17$，明文 $m=19$，公钥 $e=5$，求密文，并解密还原明文。

解　求密钥，$n=pq=7\times17=119$，$\varphi(n)=(p-1)(q-1)=6\times16=96$，根据扩展欧几里得算法计算私钥 d，d 满足 $5d\equiv1(\bmod 96)$，解得 $d=77$，则公钥$(e,n)=(5,119)$，私钥 $d=77$。

加密，对明文 $m=19$ 加密，密文 $c\equiv m^e(\bmod n)$，$c\equiv19^5\equiv66(\bmod 119)$，密文 $c=66$。

解密，收到密文 c 之后解密，明文 $m\equiv c^d(\bmod n)$，$m\equiv66^{77}\equiv19(\bmod 119)$，解密还原明文 $m=19$。

例 3.25　素数 $p=11$，$q=13$，明文 $m=24$，公钥 $e=17$，求密文，并解密还原明文。

解　求密钥，$n=pq=11\times13=143$，$\varphi(n)=(p-1)(q-1)=10\times12=120$，根据扩展欧几里得算法计算私钥 d，d 满足 $17d\equiv1(\bmod 120)$，解得 $d=113$，则公钥$(e,n)=(17,143)$，私钥 $d=113$。

加密，对明文 $m=24$ 加密，密文 $c\equiv m^e(\bmod n)$，$c\equiv24^{17}\equiv7(\bmod 143)$，密文 $c=7$。

解密，收到密文 c 之后解密，明文 $m\equiv c^d(\bmod n)$，$m\equiv7^{113}\equiv24(\bmod 143)$，解密还原明文 $m=24$。

2. 中国剩余定理用于 RSA 算法解密

在 RSA 算法中，p 和 q 为大素数，$n=pq$，$\varphi(n)=(p-1)(q-1)$，再选择整数 e 作为公钥，要求 e 与 $\varphi(n)$ 互素，即$(e,\varphi(n))=1$，求得私钥 d，满足 $ed\equiv1(\bmod \varphi(n))$。

解密时，在计算 $m\equiv c^d(\bmod n)$ 的过程中，可以利用中国剩余定理计算明文 m，等价于

解以下同余方程组：

$$\begin{cases} m \equiv c^d \pmod{p} \\ m \equiv c^d \pmod{q} \end{cases}$$

研究表明，该解法的计算量会降低到原来计算量的 25%左右。

例 3.26 计算$312^{13} \pmod{667}$。

解 根据已知条件 $n=667=23\times29$，原式可转换为以下同余方程组：

$$\begin{cases} x \equiv 312^{13} \pmod{23} \\ x \equiv 312^{13} \pmod{29} \end{cases}$$

对 $x\equiv312^{13} \pmod{23}$和 $x\equiv312^{13} \pmod{29}$利用模重复平方方法进行模幂运算(Modular Exponentiation)，上述同余方程组化简为

$$\begin{cases} x \equiv 8 \pmod{23} \\ x \equiv 4 \pmod{29} \end{cases}$$

利用中国剩余定理，解得 $m\equiv468 \pmod{667}$。

3. 模重复平方算法用于模幂运算

模幂运算也称为模指数运算，研究目的是快速计算 $b^n \pmod{m}$，该运算在公钥密码体制应用广泛。

计算 $b^n \pmod{m}$，如果直接计算，则中间结果非常大，有可能超出计算机允许的整数取值范围。例如，模运算 $165^{77} \pmod{89}$，先求 165^{77}再取模，可能中间结果就已经远远超出了计算机允许的整数取值范围，而利用模运算的性质 1.1.3：

$$(a \times c) \bmod m = (a \pmod{m} \times c \pmod{m}) \pmod{m}$$

可以极大地减小中间结果。

回顾朴素模幂运算，为避免中间结果大导致数值爆炸，可通过逐次乘法＋取模来得到最后的结果 $b^n \pmod{m}$，需要做 $n-1$ 次乘法和 $n-1$ 次模运算。然而，当幂指数较大时，耗时非常大。

现介绍模重复平方算法，该方法能有效减少计算量。

设整数 n 的二进制为 $n=(n_k n_{k-1} n_{k-2} \cdots n_2 n_1 n_0)_2$，$n_i \in \{0,1\}$，$i=0,1,2,\cdots,k$，则

$$\begin{aligned} n &= (n_k n_{k-1} n_{k-2} \cdots n_2 n_1 n_0)_2 \\ &= n_k 2^k + n_{k-1} 2^{k-1} + n_{k-2} 2^{k-2} + \cdots + n_2 2^2 + n_1 2^1 + n_0 \end{aligned}$$

故 $b^n \pmod{m}$转换为

$$\begin{aligned} b^n &\equiv b^{n_k 2^k + n_{k-1} 2^{k-1} + n_{k-2} 2^{k-2} + \cdots + n_2 2^2 + n_1 2^1 + n_0} \pmod{m} \\ &\equiv b^{n_0} \times (b^2)^{n_1} \times (b^{2^2})^{n_2} \times \cdots \times (b^{2^{k-2}})^{n_{k-2}} \times (b^{2^{k-1}})^{n_{k-1}} \times (b^{2^k})^{n_k} \pmod{m} \end{aligned}$$

从上式可以看出，当计算 b^n 时，它是 $b, b^2, b^4, b^8, \cdots, b^{2^k}$ 中某些数乘积结果。假定 n 为一个 l 位二进制数的整数，$l=\lceil \log_2 n \rceil$，所需计算的次数最多为 $2l$ 次乘法和 $2l$ 次模运算，算法复杂度为 $O(\log_2 n)$。

例如，计算 b^{22}，因为 $22=2+4+16=2+2^2+2^4$，故要计算 b^2、b^4、b^{16}的值，即

$$\begin{aligned} b^{22} &\equiv b^{1\times2^4+0\times2^3+1\times2^2+1\times2^1+0} \pmod{m} \\ &\equiv b^0 \times (b^2)^1 \times (b^{2^2})^1 \times (b^{2^3})^0 \times (b^{2^4})^1 \pmod{m} \end{aligned}$$

例 3.27 计算 $7^{22} \pmod{31}$。

解　已知 $b=7,n=22,m=31$，先计算 n 的二进制表示：

$$22=(10110)_2=2+2^2+2^4$$

然后计算 $7^2\equiv 18(\bmod 31),7^4\equiv 14(\bmod 31),7^{16}\equiv 7(\bmod 31)$，则 $7^{22}=7^{2+2^2+2^4}=7^2\times 7^{2^2}\times 7^{2^4}\equiv 18\times 14\times 7\equiv 28(\bmod 31)$。

上述计算过程，可以拆解为表 3-8 中的详细过程，本质为迭代思想。

表 3-8　例 3.27 的计算过程

i	二进制位 n_i	变量 a_i	变量 b_i
0	$n_0=0$	$a_0=ab^{n_0}(\bmod m)$	$b_1=b^2(\bmod m)$
1	$n_1=1$	$a_1=a_0b_1^{n_1}(\bmod m)$	$b_2=b_1^2(\bmod m)$
2	$n_2=1$	$a_2=a_1b_2^{n_2}(\bmod m)$	$b_3=b_2^2(\bmod m)$
3	$n_3=0$	$a_3=a_2b_3^{n_3}(\bmod m)$	$b_4=b_3^2(\bmod m)$
4	$n_4=1$	$a_4=a_3b_4^{n_4}(\bmod m)$	

初始化：令 $a=1,b=7,n=22,m=31,i=0,1,2,\cdots,k,k=\lfloor\log_2 n\rfloor=\lfloor\log_2 22\rfloor=4$。

计算完成之后，a_4 即为最后结果。

$$\begin{aligned}a_4&\equiv b^{n_0}\times b_1^{n_1}\times b_2^{n_2}\times b_3^{n_3}\times b_4^{n_4}\\&\equiv b^{n_0}\times(b^2)^{n_1}\times(b^{2^2})^{n_2}\times(b^{2^3})^{n_3}\times(b^{2^4})^{n_4}\\&\equiv b(n_4n_3n_2n_1n_0)_2(\bmod m)\end{aligned}$$

注意，因为 RSA 的加密和解密都涉及模幂运算，所以模重复平方算法既可以用于加密，也可以用于解密。

当前，针对 RSA 最流行的攻击一般是基于大整数因子分解，2009 年，编号为 RSA-768（768 位二进制数，232 位十进制数）的大整数被成功分解，为增强算法安全性，可以把 1024 位的密钥升级为 2048 位。

3.7.2　离散对数问题与 Diffie-Hellman 密钥协商算法

Diffie-Hellman 密钥协商算法实现了对称密钥的协商，其安全性基于离散对数问题（Discrete Logarithm Problem，DLP），可以解决通信双方密钥产生和传输的安全问题，多应用在安全协议或产品之中，例如，安全外壳（Security Shell，SSH）协议和安全套接层（Secure Socket Layer，SSL）协议。SSH 协议可有效防止远程管理过程中的信息泄露，SSL 协议通过加密和身份验证，可以保护服务器端和客户端之间数据传输的安全。

首先给出离散对数问题的定义。

定义 3.7.2.1　给定一个大素数 p，有限域的乘法群 $\mathbf{Z}_p^*$ 上的一个生成元 g，$g\in\mathbf{Z}_p^*$，对于任意的正整数 x，$2\leqslant x\leqslant p-2$，计算 $y\equiv g^x(\bmod p)$ 是容易的；但是反过来，已知 y、g 和 p，求 x，这个整数 x 记为 $\log_g y$，称为离散对数，满足 $y\equiv g^x(\bmod p)$ 是困难的，该问题称为**离散对数问题**。

注意，有限域的乘法群 $\mathbf{Z}_p^*$ 是循环群，其中，p 是素数。

离散对数问题也利用了单向陷门函数的原理，如图 3-4 所示。

已知 y、g 和 p，求解 x，使得 $y\equiv g^x(\bmod p)$ 通常被认为是困难的，这里“被认为是困难

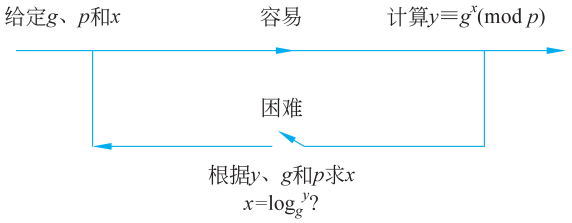

图 3-4 离散对数问题原理示意图

的”是指目前公认是困难的，也就是说，暂时没有高效的算法能在多项式时间复杂度内解决这一问题，但没人能够证明其就是困难的。

Diffie-Hellman 密钥协商算法过程如图 3-5 所示，详情如下。

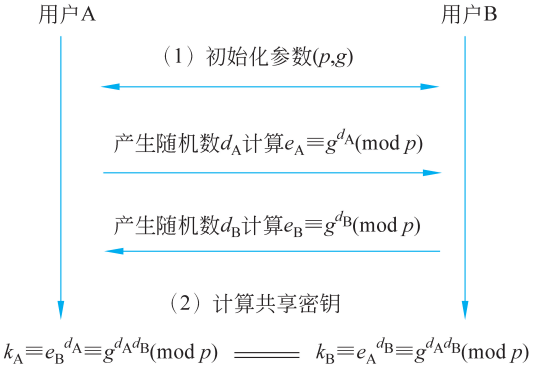

图 3-5 Diffie-Hellman 密钥协商算法过程示意图

1）初始化

① 选择一个大素数 p，计算乘法群 $\mathbf{Z}_p^*$ 上的一个生成元 g。

② 用户 A 产生一个随机数 d_A，$2\leqslant d_A\leqslant p-2$ 作为私钥，计算用户 A 的公钥 $e_A\equiv g^{d_A}(\mathrm{mod}\ p)$。

③ 用户 B 产生一个随机数 d_B，$2\leqslant d_B\leqslant p-2$ 作为私钥，计算用户 B 的公钥 $e_B\equiv g^{d_B}(\mathrm{mod}\ p)$。

2）计算共享密钥

① A 用自己的私钥 d_A 和 B 的公钥 e_B，计算共享密钥 $k_A\equiv e_B^{d_A}\equiv g^{d_Ad_B}(\mathrm{mod}\ p)$。

② B 用自己的私钥 d_B 和 A 的公钥 e_A，计算共享密钥 $k_B\equiv e_A^{d_B}\equiv g^{d_Ad_B}(\mathrm{mod}\ p)$。

可以发现，用户 A 和 B 各自产生的密钥 k_A 和 k_B 相同，都为 $g^{d_Ad_B}(\mathrm{mod}\ p)$，可以作为对称加密的密钥。第三方攻击者只能获取大素数 p、生成元 g、A 的公钥 $e_A\equiv g^{d_A}(\mathrm{mod}\ p)$ 及 B 的公钥 $e_B\equiv g^{d_B}(\mathrm{mod}\ p)$，没有私钥 d_A 和 d_B，无法求得共享密钥 $g^{d_Ad_B}(\mathrm{mod}\ p)$，这里正好利用了离散对数问题。

Diffie-Hellman 密钥协商算法在密钥建立上经常使用，同时，也能很容易地从双方密钥协商扩展到多人间的密钥协商。

例 3.28 在 Diffie-Hellman 密钥协商算法中，取素数 $p=17$，$\mathbf{Z}_p^*$ 上的一个生成元 $g=3$，用户 A 和 B 选取的随机数分别为 $d_A=15$ 和 $d_B=13$，求共享密钥。

解 首先，计算用户 A 的公钥 $e_A\equiv g^{d_A}(\mathrm{mod}\ p)$，得 $e_A\equiv 3^{15}\equiv 6(\mathrm{mod}\ 17)$，然后，计算用