

第5章

原根与指数

在研究了平方(二次)剩余之后,下面讨论 n 次剩余。

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 Euler 定理可知, 当 $(a, m) = 1$ 时, 有 $a^{\varphi(m)} \equiv 1 \pmod{m}$ 。于是, 关心一个问题, 就是这个最小的正整数 e 会不会就是 $\varphi(m)$? 什么情况下就是 $\varphi(m)$?

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

5.1

原根和阶的概念

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 $\text{ord}_m(a)$ 。

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

解答 $1^1 \equiv 1 \pmod{7}$; $2^3 \equiv 1 \pmod{7}$; $3^3 \equiv 1 \pmod{7}$;

$$4^3 \equiv (-3)^3 \equiv 1 \pmod{7}; 5^3 \equiv (-2)^3 \equiv 1 \pmod{7}; 6^2 \equiv (-1)^2 \equiv 1 \pmod{7}。$$

计算结果见表 5.1。

表 5.1 例 5.1 计算结果

a	1	2	3	4	5	6
$\text{ord}_m(a)$	1	3	6	3	6	2

容易看到, 由于 $\varphi(m) = \varphi(7) = 6$, 于是, $\text{ord}_m(a)$ 中最大为 6。

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

思考 5.1 原根的英文可能初学者觉得很难理解, 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,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)。

下面首先考察3(图5.1)。

$$\begin{aligned} 3^1 &\equiv 3 \pmod{7} & 3^2 &\equiv 2 \pmod{7} & 3^3 &\equiv 6 \pmod{7} \\ 3^4 &\equiv 4 \pmod{7} & 3^5 &\equiv 5 \pmod{7} & 3^6 &\equiv 1 \pmod{7} \end{aligned}$$

容易看到这是一个循环群,3可以生成群中的元素1~6。

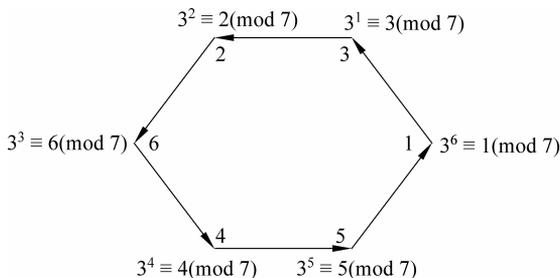


图 5.1 3 作为生成元生成 $(\mathbf{Z}/7\mathbf{Z})^*$ 中所有元素

再来考察5。

$$\begin{aligned} 5^1 &\equiv 5 \pmod{7} & 5^2 &\equiv 4 \pmod{7} & 5^3 &\equiv 6 \pmod{7} \\ 5^4 &\equiv 2 \pmod{7} & 5^5 &\equiv 3 \pmod{7} & 5^6 &\equiv 1 \pmod{7} \end{aligned}$$

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

考察2(图5.2)。

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

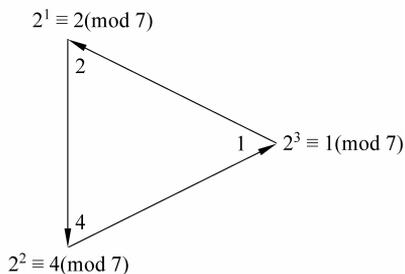


图 5.2 2 只能生成 $(\mathbf{Z}/7\mathbf{Z})^*$ 中3个元素

容易看到,2无法生成3,5,6。

看图5.1和图5.2,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。

$$\begin{aligned} \text{解答} \quad 1^1 &\equiv 1 \pmod{14} & 3^3 &\equiv -1 \pmod{14} & 5^3 &\equiv -1 \pmod{14} \\ 9^3 &\equiv 1 \pmod{14} & 11^3 &\equiv 1 \pmod{14} & 13^2 &\equiv 1 \pmod{14} \end{aligned}$$

计算结果见表 5.2。

表 5.2 例 5.2 计算结果

a	1	3	5	9	11	13
$\text{ord}_m(a)$	1	6	6	3	3	2

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

下面的定理给出了计算阶的一个算法依据。

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

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

证明 先证明充分性。如果 $\text{ord}_m(a) \mid d$, 则存在整数 k , 使得 $d = k \cdot \text{ord}_m(a)$ 。因此, 有

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

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

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

从而, 有

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

又因为

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

于是有

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

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

推论 5.1 设 $m > 1$ 是整数, a 为整数, $(a, m) = 1$, 则 $\text{ord}_m(a) \mid \varphi(m)$ 。

证明 根据 Euler 定理, 有

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

由定理 5.1, 于是 $\text{ord}_m(a) \mid \varphi(m)$ 。 ■

由推论 5.1 可知, 可以从 $\varphi(m)$ 中寻找 $\text{ord}_m(a)$ 。

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

解答 因为 $\varphi(17) = 16$, 只需要对 16 的因数 $d = 1, 2, 4, 8, 16$ 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(index)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 $x(1 \leq x \leq \varphi(m))$ 为 a 模 m 以 g 为底的指数,也称为指标或离散对数,记为 $\text{Ind}_{g,m}(a)$,或简记为 $\text{Ind}_g a$ 。^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。计算指数表。

解答 计算指数表见表 5.3。

表 5.3 例 5.4 计算结果

a	1	2	3	4	5	6
$\text{Ind}_3 a$	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 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 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

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

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, 则

- (1) 若 $b \equiv a \pmod{m}$, 则 $\text{ind}_g b \equiv \text{ind}_g a \pmod{\varphi(m)}$ 。
- (2) $\text{ind}_g 1 \equiv 0 \pmod{\varphi(m)}$ 。
- (3) $\text{ind}_g(a \cdot b) \equiv \text{ind}_g a + \text{ind}_g b \pmod{\varphi(m)}$ 。
- (4) $\text{ind}_g a^k \equiv k \cdot \text{ind}_g a \pmod{\varphi(m)}$, 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

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

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

^① 有些书籍在英译方面把 ord 译为“指数”, 而用“指标”表示离散对数。本书倾向于 ord 译为“阶”的缩写, “指数”和“指标”与离散对数等同, 缩写为 ind。

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

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

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 $x^n \equiv a \pmod{m}$ 和 $(a, m) = 1$, 可得 $(x, m) = 1$, 于是以 g 为底的 x 的对模 m 的指数存在, 设为 y , 即 $x \equiv g^y \pmod{m}$, 同余式可转化为

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

由定理 5.4 知

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

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 $4^x \equiv 16 \pmod{17}$ 所有解。

解答 两边取底为 5 模 17 的指数, 得到

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

即

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

因此

$$12x \equiv 8 \pmod{16}$$

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

$$x \equiv 14, 2, 6, 10 \pmod{16}$$

这即为同余式 $4^x \equiv 16 \pmod{17}$ 的所有解。

5.2

原根与阶的计算

不是所有的模 n 都有原根, 下面的定理给出存在原根的条件。

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

定理的证明包括以下几项。

- (1) 每个素数都有原根。
- (2) 奇素数的幂都有原根。
- (3) 2 的幂次中, 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次的 2 倍的整数才有原根。

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

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

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

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

由原根的定义知

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

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 $e | \varphi(m)$, 于是存在一个素数 q , 使得 $q | (\varphi(m)/e)$ 。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。 ■

上述定理给出了求原根算法的基础。

例 5.6 求 41 的一个原根。

解答 $\varphi(41) = 40 = 2^3 \cdot 5$, 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, ... 逐个验算:

$$\begin{array}{lll} 2^8 \equiv 10 \pmod{41} & 2^{20} \equiv 1 \pmod{41} & 3^8 \equiv 1 \pmod{41} \\ 4^8 \equiv 18 \pmod{41} & 4^{20} \equiv 1 \pmod{41} & 5^8 \equiv 18 \pmod{41} \\ 5^{20} \equiv 1 \pmod{41} & 6^8 \equiv 10 \pmod{41} & 6^{20} \equiv 40 \pmod{41} \end{array}$$

因此, 6 是模 41 的原根。

定理 5.8 设 $m > 1$ 的整数, a 为整数且 $(a, m) = 1, d \geq 0$ 为整数, 则

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

的充要条件是

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

证明 根据 Euclid 除法, 存在整数 q, r 和 q', r' 有

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

$$k = \text{ord}_m(a)q' + r' \quad 0 \leq r' < \text{ord}_m(a)$$

又 $a^{\text{ord}_m(a)} \equiv 1 \pmod{m}$, 于是

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

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

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

以上步步可逆, 知充分性。 ■

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

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

在 2.1 节中例 2.2 曾经给出一个实际的应用例子。

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

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

思考 5.3 如何利用图 5.1 和图 5.2 给出一个对上述定理的直观解释。

如图 5.3 所示, 通俗地说, 以原根 3 为度量, $2 \equiv 3^2 \pmod{7}$, 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 $\text{ord}_7(2) = 3$ 。

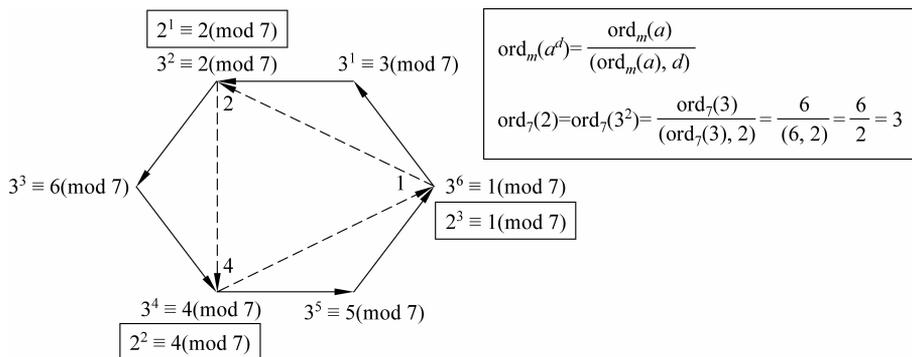


图 5.3 帮助初学者理解定理的直观解释

推论 5.2 设 $m > 1$ 是整数, g 是模 m 的原根, $d \geq 0$ 为整数, 则 g^d 是模 m 的原根当且仅当 $(d, \varphi(m)) = 1$ 。

推论 5.3 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。

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 5.9 是 41 的原根, 求 41 的所有原根。

解答 由定理 5.9 知, $(d, \varphi(41)) = 1$ 时, $\text{ord}_{41}(g^d) = \text{ord}_{41}(g)$, 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

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

综合定理 5.7 和定理 5.9, 构成了求原根的算法基础。

算法 5.1 原根算法, 输出给定素数的所有原根。

输入: 素数模 m 以及 $m - 1$ 的素因子分解 $m - 1 = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ 。

输出: m 的所有原根。

```

GetPrimitiveRoot ()
{
(1) 随机选择一个数  $a, 2 \leq a \leq m-1$ 
(2) 对  $i$  从 1 到  $k$  执行以下计算:
    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  $m-1$ , 执行以下计算:
    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 输出阶表的算法。

输入: 素数模 m , 原根 a 。

输出: 阶表。

```

GetOrder ()
{
对  $i$  从 1 到  $m-1$  执行以下计算:
    Return  $a^i \pmod{m}, (m-1)/\gcd(m-1, i)$ ;
}

```

定理 5.10 设 $m > 1$ 是整数, a 为整数且 $(a, m) = 1$, 则:

(1) 设 a^{-1} 使得 $a^{-1}a \equiv 1 \pmod{m}$, 则 $\text{ord}_m(a^{-1}) = \text{ord}_m(a)$ 。

(2) 若 $b \equiv a \pmod{m}$, 则 $\text{ord}_m(b) = \text{ord}_m(a)$ 。

证明 (1) 因为 $(a^{-1})^{\text{ord}_m(a)} \equiv (a^{\text{ord}_m(a)})^{-1} \equiv 1 \pmod{m}$

因此, $\text{ord}_m(a^{-1}) \mid \text{ord}_m(a)$ 。

同理可证 $\text{ord}_m(a) \mid \text{ord}_m(a^{-1})$, 于是有 $\text{ord}_m(a^{-1}) = \text{ord}_m(a)$ 。

(2) 若 $b \equiv a \pmod{m}$, 则

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

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

该定理结论(1)也可以从图 5.3 中有直观地解释, 3 和 5 互为逆元, 5 相当于“反着走”了一圈(图 5.4)。因为 5“走”一步到 5, 5“走”两步到 4, 依此类推, 5“走”6 步到 1。所以, 5 的阶为 6。

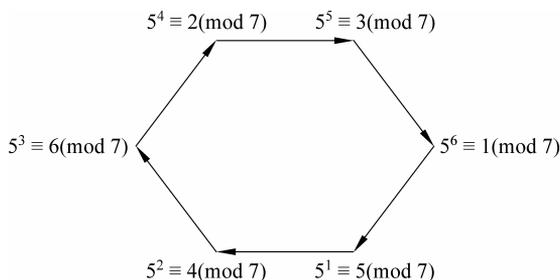


图 5.4 帮助初学者理解的对定理 5.10 的直观解释

同理,2和4互为逆元。读者也可以画个类似的示意图。

下面的定理将原根、阶以及简化剩余系等概念联系到一起。

定理 5.11 设 $m > 1$ 是整数, a 为整数且 $(a, m) = 1$, 则

$$1 = a^0, a^1, \dots, a^{\text{ord}_m(a)-1}$$

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

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

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

不妨设 $k > l$,则由 $(a, m) = 1$ 和定理 2.4,得到

$$a^{k-l} \equiv 1 \pmod{m}$$

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

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

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

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。 ■

在下一章将看到,模 m 的简化剩余系构成一个乘法群,其生成元为 a , a 生成了该群中的所有元素。这个群其实还是一个循环群。

5.3

Diffie-Hellman 密钥协商

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 DH 密钥协商协议的 ElGamal 公钥加密系统。

问题的提出:

在定义 2.7 的注解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以下两点。

(1) 密钥的管理。对称加密中加密解密双方使用相同的密钥,因此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增大。

(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的密钥,或者是通信发送方如何将密钥传递给通信接收方,都不是很容易的事情。

思考 5.5 对于共有 n 个通信方的两两通信,需要多少密钥?

对称密码需要的密钥数量:对单个个体而言,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 曾经指出,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量减少。

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。

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某种单向性(图 5.5)。

设 G 是生成元为 g 的 n 阶循环群, 则

(1) 给定整数 a , 计算元素 $g^a = y$ 是容易的。

(2) 给定 G 中元素 y , 计算整数 $x (1 \leq x \leq n)$, 使得 $g^x = y$ 通常被认为是困难的 (is believed to be hard)。

“被认为是困难的”是指目前公认是困难的, 也就是说, 目前没有高效率(如多项式时间复杂性)的算法来解决这一问题, 但没有人能够证明其就是困难的。

下面给出一个较严格的定义(需要用到第 6 章中群的概念)。

定义 5.5 乘法群 \mathbf{Z}_p^* 上的离散对数问题 (discrete logarithm problem, DLP): 给定一个素数 p , 乘法群 \mathbf{Z}_p^* 上的生成元 g , 以及 \mathbf{Z}_p^* 上的随机选取的元素 y , 寻找整数 $x (2 \leq x \leq p-2)$, 使得 $y = g^x \pmod p$ 。这个整数 x 记为 $\log_g y$, 称为离散对数。易知, \mathbf{Z}_p^* 中元素的个数为 $p-1$, 即 $\{1, 2, \dots, p-1\}$ 。

Diffie-Hellman 密钥协商协议是 2 轮协议, 即共有两个消息在信道中传递。每个通信方发送一个消息, 并接收一个消息。协议的描述如下, 如图 5.6 所示。

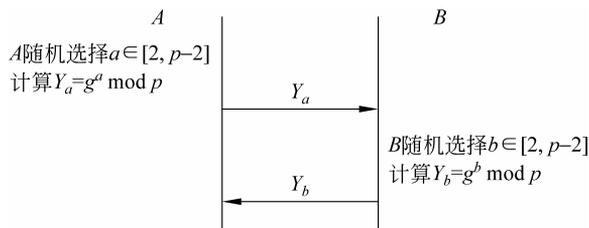


图 5.6 Diffie-Hellman 密钥协商过程

(1) A 随机选择 $a \in [2, p-2]$, 计算 $Y_a = g^a \pmod p$, 将 Y_a 发送给 B 。

(2) B 随机选择 $b \in [2, p-2]$, 计算 $Y_b = g^b \pmod p$, 将 Y_b 发送给 A 。

协议交互完成后, A 方以 $Y_b^a \pmod p$ 为密钥, B 方以 $Y_a^b \pmod p$ 为密钥。 A 方和 B 方之间的后续通信可以使用这个密钥进行加密。

例 5.9 $p=41$ 是一个素数, $(\mathbf{Z}/41\mathbf{Z})^*$ 是一个乘法循环群, 生成元为 6。

实体 A 生成随机整数 $a=6$, 计算 $Y_a = 6^6 \pmod{41} = 39$, 将 Y_a 发送给 B 。

实体 B 生成随机整数 $b=29$, 计算 $Y_b = 6^{29} \pmod{41} = 22$, 将 Y_b 发送给 A 。

A 用自己的 a 和收到的 Y_b 计算: $22^6 \pmod{41} = 21$ 。

B 用自己的 b 和收到的 Y_a 计算: $39^{29} \pmod{41} = 21$ 。

协商后的秘密密钥是 21。

为了对这个例子有更直观的理解, 图 5.7 给出一个使用计算机代数系统软件 PARI 作为演示。

思考 5.6 为什么 A 方和 B 方可以公开地协商出一个秘密的密钥?