现代密码学

第三十七讲 循环群

信息与软件工程学院

循环群

元素的方幂（乘法）

对于任意正整数n ，定义

$$a^n = \overbrace{aa\cdots a}^{n}$$

再约定

$$a^0 = e$$

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

容易验证

$$a^n a^m = a^{m+n}$$

$$(a^n)^m = a^{mn}$$

循环群

元素的方幂（加法）

对于任意正整数n，定义

$$n \times a = \underbrace{a + a + \cdots + a}_{n}$$

再约定

$$0 \times a = e$$

$$(-n) \times a = n \times a^{-1}$$

容易验证

$$n \times a + m \times a = (m+n) \times a$$

$$n \times m \times a = (mn) \times a$$

循环群

定义 1 设G 是一个群，若存在一个元素a，使得$G=\langle a\rangle$，则称G为循环群。元素 a 称为 G 的生成元。若 $o(a)=\infty$ ，G 称为无限循环群；若$o(a)=n$，n 是某个正整数，则 G 称为有限循环群。

例

（1）整数加法群 Z 是循环群，其生成元为1或-1。

（2）模整数 m 剩余类加群 Z_m 是循环群，其生成元为[1]。

（3）当m是素数时，模整数m的简化剩余类乘群 Z_m^* 是循环群。

循环群

群中的离散对数问题

定义 设 $G=\langle a\rangle$ 是循环群。群 G 中的离散对数问题是指：给定 G 中一个元素 h，找到正整数 k，使得

$$h=a^k$$

我们把 k 称为 h 相对于生成元的离散对数，记作

$$k=\log_a h$$

循环群

离散对数的例子

例 $(Z,+)$

离散对数问题是平凡的

例 Z_m，模m剩余类组成的加法群，a为 Z_m 的一个生成元，离散对数问题为：给定$h \in Z_m$ ，求解x ，使得

$$ax \equiv h \pmod{m}$$

用扩展的欧几里得算法很容易求解。

$$\log_a h = x \equiv ha^{-1} \pmod{m}$$

循环群

例 Z_m^* 是模m 简化剩余系组成的乘法群，g 为 Z_m^* 的一个生成元，离散对数问题为：给定 $h \in Z_m^*$，求解x，使得

$$g^x \equiv h \pmod m$$

当 $m=7$ 时，$\{1,2,3,4,5,6\}$ 关于模7乘法构成循环群，比如3是该群的生成元，$3^0 \equiv 1 \pmod 7, 3^1 \equiv 3 \pmod 7, 3^2 \equiv 2 \pmod 7, 3^3 \equiv 6 \pmod 7$，$3^4 \equiv 4 \pmod 7, 3^5 \equiv 5 \pmod 7, 3^6 \equiv 1 \pmod 7$

感 谢 聆 听！

xionghu.uestc@gmail.com