信息安全数学基础

循环群

熊 虎

信息与软件工程学院

xionghu.uestc@gmail.com

3.5 循环群

定义3.5.1 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3.5.1

（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）模整数m的简化剩余类乘群Z_m^*是循环群。

3.5 循环群

群中的离散对数问题

定义3.5.2 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

$$k=\log_a h$$

离散对数的例子

例3.5.2 $(Z,+)$

离散对数问题是平凡的

例3.5.3 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。

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